Science
QA
155
.D5545

DICKSON-BODEWIG

HÖHERE ALGEBRA

LEIPZIG / B. G. TEUBNER / BERLIN

Digitized by Google
Original from
UNIVERSITY OF MICHIGAN

Berichtigungen.

Seite 6 letzte Zeile von Beispiel 10: lies L statt l.
,, 32 Zeile 3 von unten: lies $pU + qV$ statt $pU + gV$.
,, 33 a) Zeile 2: lies $l - n$ statt $i - n$.
b) zweite Zeile unter (15): lies z_m statt z_{m+1}.
,, 62 Zeile unter (14): lies x_k statt x_k.
,, 95 unterste Zeile: lies $d_1 d_3 d_4$ statt $d_1 d_2 d_3$.
,, 102 Zeile 17: lies PJP^{-1} statt $P^{-1}JP$.
,, 103 Zeile 5 von unten: lies $|\varrho M + \sigma N|$ statt $\varrho M + \sigma N$.
,, 107 zweite Zeile unter (5): lies $\varrho\mu + \sigma\nu$ statt $\varrho\mu + \sigma r$.
,, 130 a) zweite Zeile über Satz 5: lies $x_{m_i+\alpha}$ statt $x_{m_i} + \alpha$.
b) $y_{m_i+\alpha}$ statt $y_{m_i} + \alpha$.
,, 162 Zeile 10 von unten: lies ψ_i statt φ_i.
,, 170 Zeile 1: lies Satz 9 statt Satz 5.
,, 179 a) Zeile 5: lies $v_i^{\overset{1}{\mu}}$ statt $v^{\overset{1}{\mu}}$.
b) Zeile 8 unter § 108: lies ϱ^{28} statt ϱ^{47}.
,, 211 zweite Zeile über (39): lies $f^5 - Z \cdot J^2$ statt $f^5 + Z \cdot J^2$.
,, 228 in (8): lies im Summenzeichen s_g statt S_g.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

HÖHERE ALGEBRA

AUTORISIERTE DEUTSCHE AUSGABE VON

L. E. DICKSON „MODERN ALGEBRAIC THEORIES"

HERAUSGEGEBEN VON

EWALD BODEWIG
KÖLN A. RH.

MIT 3 FIGUREN

1929
LEIPZIG UND BERLIN
VERLAG UND DRUCK VON B. G. TEUBNER

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Math.-Econ.
Library

QA
155
.D5545

Digitized by Google

Original from
UNIVERSITY OF MICHIGAN

Math-Econ
Math
Stechert
12.20.54
90373

VORWORT DES VERFASSERS ZUR DEUTSCHEN AUSGABE.

Die Originalausgabe dieses Buches (Modern Algebraic Theories, B. H. Sanborn & Co., 1926) fand bei den englischen Lesern eine so günstige Aufnahme, daß der Verfasser sich dem Vorschlag einer deutschen Übersetzung nicht verschließen konnte. Die ursprüngliche Ausgabe wurde jedoch nicht unverändert übernommen, sondern um ein Kapitel verkürzt und dafür um das so wichtige Kapitel über Paare von bilinearen und quadratischen Formen im singulären Falle erweitert.

12-31-54 MFP

Das Ziel des Buches ist eine einfache Einführung in die Hauptdisziplinen der höheren Algebra. Die Theorie der linearen Algebren (Theorie der höheren komplexen Zahlen) ist Gegenstand eines anderen Werkes des Verfassers (Algebren und ihre Zahlentheorie, Orell Füssli, Zürich 1927).

Die beiden ersten Kapitel behandeln die Theorie der projektiven Invarianten mit Hilfe der unsymbolischen Methode. Sie schließen mit dem Hilbertschen Endlichkeitsbeweis für binäre Formen.

Kapitel III—VII enthalten eine elementare Einführung in die Theorie der Matrizen, linearen Transformationen, Elementarteiler und invarianten Faktoren sowie der quadratischen, bilinearen und Hermiteschen Formen und Formenpaare unter besonderer Berücksichtigung der Rationalitätsfragen. Die Elementarteiler und invarianten Faktoren ergeben sich in Kapitel V auf natürliche Weise aus der klassischen und einer neuen rationalen kanonischen Form der linearen Transformationen, eine Einführung, die nicht nur viel elementarer ist als die sonst gebräuchliche, sondern die auch in engerer Verbindung mit den Anwendungen steht. So ergeben sich in Kapitel VI die Kriterien für die Äquivalenz von Paaren bilinearer oder quadratischer Formen als bloße Folgerungen.

Die Kapitel VIII—XII behandeln die Galoissche Theorie und das Wichtigste aus der Gruppentheorie mit der Einfachheit, aber auch mit der Strenge, welche diese wichtigen Gegenstände erfordern. Die Darstellung gipfelt in der Beantwortung der Fragen:

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Ist jede Gleichung auflösbar? Kann jeder Winkel mit Zirkel und Lineal in drei gleiche Teile geteilt werden? Welche regulären Polygone können elementar konstruiert werden?

Kleins „Vorlesungen über das Ikosaeder" und über die Gleichungen fünften Grades gehören zu unserer klassischen Literatur; dem Anfänger bereiten sie jedoch durch die aus vielen Teilen der höheren Mathematik entlehnten Begriffe nicht geringe Schwierigkeiten. Die Grundzüge dieser wichtigen und interessanten Theorie sind in Kapitel XIII auf einfache Weise auseinandergesetzt. Als Fortsetzung davon enthält das Schlußkapitel die Hauptresultate über die Darstellung einer Gruppe als lineare Gruppe und der Frobeniusschen Theorie der Gruppencharaktere.

Chicago, im September 1928. **L. E. Dickson.**

VORWORT DES ÜBERSETZERS.

Das Dicksonsche Buch schien mir in seiner vorstehend gekennzeichneten Eigenart den bei uns vorhandenen Lehrbüchern gegenüber als Einführung in die höhere Algebra so große Vorzüge zu bieten, daß ich dem Verlag mit gutem Gewissen seine Übersetzung empfehlen zu können glaubte. Man neigt bei uns meistens noch zu einer von Anfang an so abstrakten und systematischen Darstellung — vor allem bei der Galoisschen Theorie —, daß dadurch mancher Anfänger den Mut verliert. Die Forderung nach genetischen Beweisen hat sich in Lehrbüchern noch nicht durchgesetzt. Und gerade diese didaktischen Dinge sind es, die das Dicksonsche Buch so betont: seine elementare, genetische Darstellung und ganz besonders auch die vielen Beispiele und Übungen werden den Lernenden mancher Schwierigkeit entheben. Daneben ist natürlich auch rein sachlich vieles von dem Inhalt der gebräuchlichen Lehrbücher verschieden, so z. B. das Kapitel über die Formenpaare im singulären Falle, das in den Kroneckerschen Originalabhandlungen so schwer lesbar ist. Auch eine so knappe und inhaltsreiche Darstellung der Invariantentheorie wird man in deutschen Büchern vergeblich suchen. — Die mathematische Ausdrucksweise wurde an einigen Stellen, wo sie sich von der in Deutschland üblichen unterschied, bei der Übersetzung entsprechend geändert.

Köln, im Januar 1929. **E. Bodewig.**

Digitized by Google Original from UNIVERSITY OF MICHIGAN

INHALTSVERZEICHNIS.

Seite

Vorwort III

Erstes Kapitel. Einführung in die Theorie der algebraischen Invarianten 1

Lineare Transformationen 1. — Hessesche Form 2. — Invarianten und Kovarianten 4. — Funktionaldeterminanten 5. — Kanonische Form einer kubischen und biquadratischen Form. Lösung der kubischen und biquadratischen Gleichung 8. 18. — Homogeneität 9. — Gewicht 10. — Seminvarianten 12. — Vollständiges System einer binären p-ik für $p < 5$ 15. — Geometrische Anwendungen 20.

Zweites Kapitel. Fortführung der Theorie der Kovarianten binärer Formen 23

Annihilatoren 23. — Kommutatoren 26. — Existenzbeweis für eine Kovariante mit gegebenen seminvariantem Leitgliede 27. — Der Hilbertsche Satz 28. — Endlichkeit des Formensystems 30. — Endlichkeit der Syzygien 33. — Kanonische Form einer binären Form ungrader Ordnung 34. — Weitere Probleme 36.

Drittes Kapitel. Matrizen, Bilineare Formen, Lineare Gleichungen . 37

Lineare Formen, Matrizen, Lineare Transformationen 37. — Inverse und adjungierte Matrix 39. — Assoziatives und distributives Gesetz 41. — Charakteristische Gleichung 43. — Rang 45. — Bilineare Formen 47. — Körper 48. — Lineare Unabhängigkeit 49. — Äquivalenz von Matrizen 52. — Lineare Gleichungen 55.

Viertes Kapitel. Quadratische und Hermitesche Formen. Symmetrische und Hermitesche bilineare Formen 58

Symmetrische bilineare und quadratische Formen 58. — Hermitesche und Hermitesche bilineare Formen 60. — Rationale Reduktion quadratischer und Hermitescher Formen 62. — Kanonische Formen 64. — Orthogonale Transformationen 66. — Rang einer symmetrischen und Hermiteschen Matrix 70. — Die Kroneckersche Reduktionsmethode 74. — Größe des Index in der kanonischen Form 78.

Fünftes Kapitel. Theorie der linearen Transformationen. Invariante Faktoren und Elementarteiler 80

Rationale kanonische Form einer linearen Transformation 80. — Invariante Faktoren 88. — Drehungen und orthogonale Transformationen 89. — Eindeutige Bestimmtheit der kanonischen Form durch ihre invarianten Faktoren 93. — Ähnliche Transformationen 93. — Klassische kanonische Form 94. — Elementarteiler 98.

Digitized by Google

Original from UNIVERSITY OF MICHIGAN

Seite

Sechstes Kapitel. Paare von bilinearen und quadratischen Formen 101

Äquivalenz von Matrizenpaaren 101. — Kanonische Form eines Paares bilinearer Formen 104. — Formenbüschel 107. — Die $n$ten Wurzeln einer Matrix 107. — Äquivalenz von Paaren quadratischer Formen 109. — Paare mit alternierenden Formen 111. — Das Weierstraßsche kanonische Paar 112.

Siebentes Kapitel. Paare von bilinearen und quadratischen Formen im singulären Falle 115

Paare von bilinearen Formen 115. — Minimalgradzahlen 127. — Paare symmetrischer bilinearer Formen 129. — Paare quadratischer Formen 131. — Weitere Anwendungen der Matrizentheorie 131.

Achtes Kapitel. Haupteigenschaften der Substitutionsgruppen . . . 133

Kubische und biquadratische Gleichungen 133. 139. — Ihre Diskriminanten 135. 139. — Substitutionen 136. — Gruppen 140. — Gruppe, die eine Funktion ungeändert läßt 141. — Alternierende Gruppe 142. — Untergruppe 144.

Neuntes Kapitel. Körper. Reduzible und irreduzible Funktionen . 145

Der größte gemeinsame Teiler 146. — Das Gaußsche Lemma 149. — Irreduzibilität der Kreisteilungsgleichung 150.

Zehntes Kapitel. Gruppe einer Gleichung in einem gegebenen Körper 152

Galoissche Resolventen 154. — Eigenschaften der Galoisschen Gruppe 156. — Transitive und reguläre Gruppen 158. — Rationale Funktionen, die zu einer Gruppe gehören 161. — Erniedrigung der Gruppe 164. — Gruppe der allgemeinen Gleichung 165. — Weitere Ergebnisse 165.

Elftes Kapitel. Auflösbare Gleichungen 168

Historisches 168. — Resolventengleichungen 169. — Invariante Untergruppen 173. — Transformierte einer Substitution 174. — Einfache und Quotientengruppen 175. — Kompositionsreihen. Auflösbare Gruppen 176. — Zyklische Gleichungen 178. — Kreisteilungsgleichungen 179. — Sätze von Jordan und Galois 183. — Auflösbarkeit 185.

Zwölftes Kapitel. Konstrukionen mit Zirkel und Lineal 191

Analytisches Kriterium für die Konstruierbarkeit 191. — Dreiteilung des Winkels 193. — Reguläre Polygone 194.

Dreizehntes Kapitel. Polyedergruppen. Gleichungen fünften Grades 196

Die einer Drehung zugeordnete lineare Transformation 196. — Tetraeder-, Oktaeder-, Ikosaedergruppe; ihre Invarianten und Formenprobleme 198. — Brioschiche Normalform. Resolvente der Ikosaeder-

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Seite

gleichung 214. — Gleichung fünften Grades 219. — Galoissche Gruppe der Ikosaedergleichung 220. — Weitere Ergebnisse 221.

Vierzehntes Kapitel. Darstellung einer endlichen Gruppe als lineare Gruppe. Gruppencharaktere 223

Reduzible lineare Gruppen 223. — Darstellung 225. — Reduzible und irreduzible Gruppenmatrizen 227. — Reguläre Gruppenmatrix 233. — Gruppencharaktere und ihre Anwendungen 235. — Die alternierende Gruppe von 5 Elementen 238.

Sachverzeichnis 240

Namenverzeichnis 242

Digitized by Google

Original from UNIVERSITY OF MICHIGAN

Digitized by Google
Original from
UNIVERSITY OF MICHIGAN

ERSTES KAPITEL.

EINFÜHRUNG IN DIE THEORIE DER ALGEBRAISCHEN INVARIANTEN.

Invarianten und Kovarianten spielen in allen Teilen der Mathematik eine wichtige Rolle. Dieses Kapitel enthält das Notwendigste der *projektiven* Invariantentheorie. Es behandelt ziemlich ausführlich die Theorie der Invarianten und Kovarianten eines in x und y homogenen Polynoms von niederem als fünftem Grade und enthält eine Anwendung auf die Lösung der kubischen und biquadratischen Gleichung. Bei höherem als viertem Grade sind die meisten Kovarianten zu kompliziert gebaut und daher, wenn man sie nicht gerade in ihrer symbolischen Darstellung verwendet, nur von geringem Nutzen.

1. **Lineare Transformationen.** Beziehungen der Form

$$x = a\xi + b\eta, \quad y = c\xi + d\eta, \quad \text{wo} \quad D = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0,$$

welche zwei Paar von Veränderlichen, hier x, y und ξ, η miteinander verbinden, definieren eine lineare Transformation T mit der Determinante D. Nehmen wir eine andere lineare Transformation U hinzu von der Form

$$\xi = eX + fY, \quad \eta = gX + hY, \quad \text{wo} \quad \Delta = \begin{vmatrix} e & f \\ g & h \end{vmatrix} \neq 0,$$

so erhält man durch Elimination von ξ und η die Gleichungen

$$x = kX + lY, \quad y = mX + nY,$$

welche wieder eine lineare Transformation P definieren, die man das „Produkt" von T und U (in dieser Reihenfolge genommen!) nennt und mit TU bezeichnet. Die Werte der Koeffizienten sind

$$k = ae + bg, \quad l = af + bh, \quad m = ce + dg, \quad n = cf + dh.$$

Die Determinante von P ist $D\Delta$ und daher von Null verschieden.

Wenn wir die zu T gehörigen Gleichungen auflösen und im Ergebnis x durch X und y durch Y ersetzen, so bekommen wir

$$\xi = D^{-1}dX - D^{-1}bY, \quad \eta = -D^{-1}cX + D^{-1}aY.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Diese Gleichungen definieren eine Transformation, welche die inverse von T heißt und mit T^{-1} bezeichnet wird. Das Produkt TT^{-1} findet man aus den vorherigen Gleichungen durch Elimination von ξ und η und erhält: $x = X$, $y = Y$. Sie heißt die identische Transformation. — Ähnlich zeigt man, daß auch $T^{-1}T$ die identische Transformation ergibt.

Wir werden nun die Gültigkeit des assoziativen Gesetzes

$$T \cdot UV = TU \cdot V$$

beweisen, die es uns erlaubt, jedes dieser Produkte mit TUV zu bezeichnen. Denn wenn

$$X = pu + qv, \quad Y = ru + sv$$

die zu V gehörigen Gleichungen sind, so findet man das Produkt $TU \cdot V$, indem man zuerst ξ, η und dann X, Y zwischen den obigen Gleichungen eliminiert, während man das Produkt $T \cdot UV$ erhält, indem man erst X, Y und dann ξ, η eliminiert. In jedem Falle müssen wir aber offenbar dieselben Gleichungen erhalten, die x und y als lineare Funktionen von u und v ausdrücken.

2. Formen und ihre Einteilung. Ein Polynom wie

$$ax^3 + bx^2y + cxyz + dxz^2,$$

dessen Glieder alle dieselbe Gesamtordnung (hier 3) in den Variablen (hier x, y, z) haben, wird homogen in den Variablen genannt. Ein homogenes Polynom heißt eine Form. Je nachdem die Zahl der Variablen 1, 2, 3, 4, ... allgemein n ist, heißt die Form unär, binär, ternär, quaternär, ... allgemein n är oder von der Stufe n. Je nachdem die Form den Grad 1, 2, 3, 4, ..., p hat, heißt sie linear, quadratisch, kubisch, biquadratisch, ..., allgemein vom Grade (Ordnung) p oder eine p-ik (sprich Pe-ik).

Z. B. ist obiges Polynom eine ternäre kubische, während $ax^2 + bxy + cy^2$ eine binäre quadratische Form ist.

3. Die Hessesche Form. Die Hessesche Form (benannt nach Otto Hesse) einer Funktion $f(x, y)$ von zwei Variablen ist die Determinante

$$(1) \qquad \begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{vmatrix},$$

deren Elemente die zweiten partiellen Ableitungen sind. Z. B. ist die Hessesche Form von $f = ax^2 + 2bxy + cy^2$ gleich $4(ac - b^2)$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Hessesche Form h von $f(x_1, x_2, \ldots, x_q)$ ist die Determinante $q$ter Ordnung, deren Elemente in der $i$ten Reihe

$$\frac{\partial^2 f}{\partial x_i \partial x_1}, \frac{\partial^2 f}{\partial x_i \partial x_2}, \ldots, \frac{\partial^2 f}{\partial x_i \partial x_q} \tag{2}$$

sind. Wir wollen nun untersuchen, wie sich diese Determinante ändert, wenn die Variablen x der Transformation

$$x_i = c_{i1} y_1 + \cdots + c_{iq} y_q \qquad (i = 1, 2, 3, \ldots, q) \tag{3}$$

mit der Determinante $\Delta = \begin{vmatrix} c_{11}, \ldots, c_{1q} \\ \vdots \\ c_{q1}, \ldots, c_{qq} \end{vmatrix}$

unterworfen werden. f werde dabei zu $F(y_1, y_2, \ldots, y_q)$. Das Produkt $h\Delta$ ist eine Determinante $q$ter Ordnung, deren Element in der $i$ten Reihe und $k$ten Spalte gleich ist der Summe der Produkte der Elemente (2) der $i$ten Reihe von h und der entsprechenden Elemente $c_{1k}, c_{2k}, \ldots, c_{qk}$ der $k$ten Spalte von Δ und daher auch gleich ist der partiellen Ableitung von

$$\begin{aligned} &\frac{\partial f}{\partial x_1} c_{1k} + \frac{\partial f}{\partial x_2} c_{2k} + \cdots + \frac{\partial f}{\partial x_q} c_{qk} \\ &\qquad = \frac{\partial f}{\partial x_1} \cdot \frac{\partial x_1}{\partial y_k} + \frac{\partial f}{\partial x_2} \frac{\partial x_2}{\partial y_k} + \cdots + \frac{\partial f}{\partial x_q} \cdot \frac{\partial x_q}{\partial y_k} = \frac{\partial F}{\partial y_k} \end{aligned} \tag{4}$$

in bezug auf x_i. Jetzt bezeichne Δ' die Determinante, die man aus Δ durch Vertauschung von Reihen und Spalten erhält, so daß $\Delta' = \Delta$. Dann ist in dem Produkt $\Delta' \cdot h\Delta$ das Element der $r$ten Reihe und $k$ten Spalte gleich

$$c_{1r} \frac{\partial}{\partial x_1} \frac{\partial F}{\partial y_k} + \cdots + c_{qr} \frac{\partial}{\partial x_q} \frac{\partial F}{\partial y_k} = \frac{\partial}{\partial y_r} \cdot \frac{\partial F}{\partial y_k},$$

da c_{iq} die partielle Ableitung von x_i in (3) nach y_r ist. Daraus folgt, daß

$$\Delta^2 h = \left| \frac{\partial^2 F}{\partial y_r \partial y_k} \right|_{r, k = 1 \ldots q},$$

also gleich der Hesseschen Form von F ist.

Satz 1: Wenn F die Funktion bedeutet, die aus f durch eine lineare Transformation mit der Determinante Δ hervorgeht, so ist die Hessesche Form von F gleich dem Produkt der Hesseschen Form von f und Δ^2.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

4. Definition von Invarianten und Kovarianten. Eine Transformation T mit der Determinante Δ, welche x und y linear durch ξ und η ersetzt, möge $f = ax^2 + 2bxy + cy^2$ überführen in $A\xi^2 + 2B\xi\eta + C\eta^2$. In 3. sahen wir, daß die Hessesche Form von f gleich dem Vierfachen der Diskriminante $ac - b^2$ von f ist, also nach Satz 1

$$AC - B^2 = \Delta^2(ac - b^2).$$

Wir nennen $ac - b^2$ eine Invariante von f vom Gewicht 2. Diese Definition läßt sich folgendermaßen verallgemeinern:

Die allgemeine binäre Form $p$ter Ordnung

$$f = a_0x^p + a_1x^{p-1}y + \cdots + a_py^p$$

werde durch die Transformation T in

$$F = A_0\xi^p + A_1\xi^{p-1}\eta + \cdots + A_p\eta^p$$

übergeführt. Ein Polynom $I(a_0, a_1, \ldots, a_p)$ heißt nun eine Invariante von f vom Gewicht l, wenn für jede Transformation T mit nichtverschwindender Determinante Δ

$$I(A_0, A_1, \ldots, A_p) = \Delta^l \cdot I(a_0, a_1, \ldots, a_p)$$

(identisch in $a_0, \ldots, a_p$, wenn die A durch ihre Ausdrücke in den a ersetzt werden).

Ähnlich werden Kovarianten definiert. Wenn für jede Transformation T (mit $\Delta \neq 0$) ein Polynom K in den Koeffizienten und Variabeln von f die Eigenschaft hat, daß

$$K(A_0, A_1, \ldots, A_p; \xi, \eta) \equiv \Delta^g \cdot K(a_0, a_1, \ldots, a_p; x, y)$$

(identisch in $a_0, \ldots, a_p$, ξ, η, wenn die A durch ihre Ausdrücke in den a und x und y durch ihre Ausdrücke in ξ und η ersetzt werden), so heißt K eine Kovariante von f vom Gewichte g.

Nach Satz 1 ist die Hessesche Form von f eine Kovariante von f vom Gewicht 2. Man beachte, daß f selbst eine Kovariante von f vom Gewichte Null ist, da $F = \Delta^0 \cdot f$.

Unter einer Kovariante vom Gewichte g eines Systems von Formen $f_1, f_2, \ldots, f_k$ versteht man eine solche Funktion ihrer Koeffizienten und Variablen $x_1, x_2, \ldots, x_q$, die, mit Δ^g multipliziert, den gleichen Wert annimmt wie dieselbe Funktion der entsprechenden Koeffizienten und Variabeln $y_1, y_2, \ldots, y_q$ der Formen $F_1, \ldots, F_k$, die aus $f_1, \ldots, f_k$ durch eine nichtsinguläre Transformation (d. h. eine Transformation mit $\Delta \neq 0$) hervorgehen. — Ein Beispiel wird unten durch Satz 2 gegeben.

Eine Kovariante, die keine einzige Variable enthält, ist eine Invariante.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

5. Funktionaldeterminanten. Die Funktionaldeterminante oder Jacobische Form (benannt nach C. G. J. Jacobi) von q Funktionen $f_1(x_1, \ldots, x_q), \ldots, f_q(x_1, \ldots, x_q)$ in bezug auf die Variabeln $x_1, \ldots, x_q$ wird durch die Determinante

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} \cdots \frac{\partial f_1}{\partial x_q} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \frac{\partial f_q}{\partial x_1} & \frac{\partial f_q}{\partial x_2} \cdots \frac{\partial f_q}{\partial x_q} \end{vmatrix} \tag{5}$$

definiert.

Satz 2: Die Funktionaldeterminante von $f_1, \ldots, f_q$ ist eine Kovariante des Systems $f_1, \ldots, f_q$ vom Gewichte Eins.

Die Transformation (3) mit der Determinante Δ möge f_i überführen in $F_i(y_1, \ldots, y_q)$. Dann besteht die Beziehung (4), wenn wir an jedes f und F den Index i anfügen. Daher ist die Funktionaldeterminante von $F_1, \ldots, F_q$ in bezug auf die Variabeln $y_1, \ldots, y_q$ gleich

$$\begin{vmatrix} \frac{\partial f_1}{\partial x_1} c_{11} + \cdots + \frac{\partial f_1}{\partial x_q} c_{q1}, \ldots, \frac{\partial f_1}{\partial x_1} c_{1q} + \cdots + \frac{\partial f_1}{\partial x_q} c_{qq} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \frac{\partial f_q}{\partial x_1} c_{11} + \cdots + \frac{\partial f_q}{\partial x_q} c_{q1}, \ldots, \frac{\partial f_q}{\partial x_1} c_{1q} + \cdots + \frac{\partial f_q}{\partial x_q} c_{qq} \end{vmatrix}$$

Diese Determinante ist aber das Produkt der Determinante (5) und der Determinante $\Delta = |c_{ik}|$.

Übungen: 1. Wenn $f_1, \ldots, f_q$ voneinander abhängen, so verschwindet ihre Funktionaldeterminante identisch. (Man setze $f_q = g(f_1, \ldots, f_{q-1})$ und wende den Abhängigkeitssatz der Determinantentheorie an.)

2. Zwei Funktionen f und g von x und y sind voneinander abhängig, wenn ihre Funktionaldeterminante J identisch verschwindet.

[Abgesehen von dem Fall, wo g eine konstante Funktion von x ist, können wir $\frac{\partial g}{\partial x}$ als nichtidentisch Null annehmen und daher x als Funktion von g und y voraussetzen. Dann wird $f = F(g, y)$ und $J = -\frac{\partial g}{\partial x} \cdot \frac{\partial F}{\partial y}$. Soll dies identisch verschwinden, so muß $f = F(g)$ sein.]

3. Wenn $f(x, y)$ eine binäre Form $p$ter Ordnung ist, so ist (nach Euler)

$$x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y} \equiv p \cdot f.$$

4. Die Hessesche Form von $(ax + by)^p$ verschwindet identisch. (Warum genügt es, dies für x^p zu beweisen?)

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

5. Umgekehrt: Wenn die Hessesche Form einer binären Form $f(x, y)$ von der Ordnung p identisch verschwindet, so ist f die $p$te Potenz einer Linearform.

(Die Hessesche Form von f ist die Jacobische von $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}$. Letztere Funktionen sind nach 2 abhängig voneinander. Daher ist $b\frac{\partial f}{\partial x} - a\frac{\partial f}{\partial y} = 0$, wo a und b Konstanten sind. Man bestimme aus dieser Gleichung und aus der Eulerschen Beziehung $\frac{\partial f}{\partial x}$ und $\frac{\partial f}{\partial y}$, bestimme die Ableitungen von $\log f$ und integriere.)

6. Wenn die Funktionaldeterminante einer quadratischen Form f und einer linearen Form h in x und y identisch verschwindet, so ist (abgesehen von einem Zahlenfaktor) f gleich h^2.

7. Wenn eine Form in q Variabeln als eine Form in weniger als q Variabeln darstellbar ist, so verschwindet ihre Hessesche Form identisch.[1])

8. Die Funktionaldeterminante einer binären Form f und ihrer Hesseschen Form h ist eine Kovariante von f vom Gewichte 3.

9. $f = ax^2 + 2bxy + cy^2$ und $g = px^2 + 2qxy + ry^2$ haben die Invariante $s = ar - 2bq + cp$ vom Gewichte 2.

(Denn die Diskriminante von $f + tg$ ist für jeden Wert von t eine Invariante.)

10. Eine binäre quadratische Form f und eine lineare Form L haben eine lineare Kovariante J, ihre Funktionaldeterminante. Man zeige, daß die Funktionaldeterminante von J und L eine Invariante vom Gewichte 2 des Systems f und $\mathfrak{L}$ ist.

11. Man beweise, daß die durch $f = 0$ dargestellten Punkte von den durch $L = 0$ und $J = 0$ dargestellten Punkten harmonisch getrennt werden. (Vgl. Beispiel 10.)

6. Die Diskriminante einer binären kubischen Form. Es sei

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3. \tag{6}$$

Ihre Hessesche Form ist $36h$, wo

$$h = rx^2 + 2sxy + ty^2,\ r = ac - b^2,\ 2s = ad - bc,\ t = bd - c^2. \tag{7}$$

Durch eine lineare Transformation mit der Determinante Δ möge f übergehen in

$$F = A\xi^3 + 3B\xi^2\eta + 3C\xi\eta^2 + D\eta^3. \tag{8}$$

1) Die Umkehrung gilt nicht allgemein (wie Hesse irrtümlich glaubte), sondern nur für $q < 5$. Vgl. Gordan und Noether, Math. Annalen 10, 1876, p. 564.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Man bezeichne die Hessesche Form von F mit $36H$. Da h eine Kovariante von f vom Gewichte 2 ist, so ist

$$(9)\qquad \begin{aligned} H &= R\xi^2 + 2S\xi\eta + T\eta^2 = \Delta^2 \cdot h, \\ R &= AC - B^2,\ 2S = AD - BC,\ T = BD - C^2. \end{aligned}$$

Daher sind $\Delta^2 r, 2\Delta^2 s, \Delta^2 t$ die Koeffizienten einer binären quadratischen Form, welche durch unsere Transformation in eine solche mit den Koeffizienten $R, 2S, T$ übergeht. Da die Diskriminante einer binären quadratischen Form eine Invariante vom Gewichte 2 ist, so bekommt man

$$RT - S^2 = \Delta^2[\Delta^2 r \cdot \Delta^2 t - (\Delta^2 s)^2] = \Delta^6(rt - s^2).$$

Daher[1]) ist $rt - s^2$ eine Invariante von f vom Gewichte 6. Wir werden

$$(10)\qquad -4(rt - s^2) = (ad - bc)^2 - 4(ac - b^2)(bd - c^2)$$

die Diskriminante der binären kubischen Form (6) nennen.

Der Name „Diskriminante" erhält seine Rechtfertigung durch

Satz 3: Das Verschwinden der Invariante (10) *ist notwendig und hinreichend dafür, daß* $f\left(\frac{x}{y}, 1\right) = 0$ *eine mehrfache Wurzel hat, d. h. daß* $f(x, y)$ *durch das Quadrat einer linearen Funktion von* x *und* y *teilbar ist.*

Angenommen, letzteres sei der Fall, so können wir f in eine Form wie (8) transformieren, die den Faktor ξ^2 besitzt. Dann ist $C = D = 0$ und die Funktion (10), in großen Buchstaben geschrieben, verschwindet, so daß auch die Invariante (10) selbst gleich Null wird.

Umgekehrt sei vorausgesetzt, daß (10), also auch die Diskriminante von (7) verschwindet. Dann ist h das Quadrat einer linearen Funktion ξ. Man übe eine lineare Transformation aus, die x und y durch ξ und irgendeine davon unabhängige Funktion η ausdrückt. Jetzt ist wegen $h = \xi^2$ in (9) $S = T = 0$. Wenn nun $D = 0$, so verschwindet wegen $T = 0$ auch C, und (8) hat den Faktor ξ^2. — Ist hingegen $D \neq 0$, so haben wir

$$B = \frac{C^2}{D},\quad A = \frac{C^3}{D^2},\quad F = D\left(\eta + \frac{C}{D}\xi\right)^3.$$

1) Dieses Ergebnis und die Beispiele 8 und 10 von 5. erläutern den Satz, daß jede Invariante (oder Kovariante) einer oder mehrerer Kovarianten eines Systems von Formen eine Invariante (oder Kovariante) der Urformen ist.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

In beiden Fällen ist $f = F$ durch das Quadrat einer linearen Funktion teilbar.

7. Kanonische Form einer binären kubischen Form. Lösung der kubischen Gleichung.

Satz 4: Jede binäre kubische Form kann auf die Gestalt $X^3 + Y^3$ gebracht werden, wenn ihre Diskriminante von Null verschieden ist, im anderen Fall auf die Gestalt $X^2 Y$ oder auf die Gestalt X^3.

Da die letzte Behauptung bewiesen ist, so sei die Diskriminante (10) der Form (6) von Null verschieden. Unterdrücken wir bei ~~bei~~ allen Hesseschen Formen den Faktor 36, so ist die Hessesche Form (7) das Produkt zweier linear unabhängiger Faktoren ξ und η. Daher kann f in eine Form F von der Gestalt (8) transformiert werden, deren Hessesche Form (9) sich auf $2S\xi\eta$ reduziert, so daß $R = 0$, $T = 0$, $S \neq 0$. Ist nun $C = 0$, so verschwindet wegen $R = 0$ auch B, und es ist $F = A\xi^3 + D\eta^3$, wo wegen $S \neq 0$ auch $AD \neq 0$. Setzt man jetzt noch

$$\xi = A^{-\frac{1}{3}} X, \quad \eta = D^{-\frac{1}{3}} Y,$$

so bekommen wir die gewünschte Gestalt $F = X^3 + Y^3$. Der übrigbleibende Fall $C \neq 0$ wird bald als unmöglich erkannt; denn es wäre dann wegen $T = 0$, $B \neq 0$ und

$$A = \frac{B^2}{C}, \quad D = \frac{C^2}{B}, \quad \text{also} \quad AD = BC \quad \text{und} \quad S = 0.$$

Um daher eine kubische Gleichung $c(w) = 0$, die keine mehrfache Wurzel hat, zu lösen, bestimme man die Faktoren ξ und η der Hesseschen Form von f und bringe die kubische Form $f(x, y) \equiv y^3 c\left(\frac{x}{y}\right)$ auf die Gestalt $A\xi^3 + D\eta^3$. Die dann entstehende rein kubische Gleichung besitzt die Wurzeln $\omega\sqrt[3]{-\frac{D}{A}}$, wo ω eine 3. Einheitswurzel ist.

Übungen: 1. Die Hessesche Form von $f = x^3 + 6x^2y + 12xy^2 + dy^3$ ist $36(d - 8)(xy + 2y^2)$. Wenn ihre Faktoren $\xi = x + 2y$ und $\eta = y$ als neue Variabeln eingeführt werden, wird $f = \xi^3 + (d - 8)\eta^3$.

2. Ist in Beispiel 1 $d = 9$, so wird $\frac{x}{y} = -3;\ -2 - \omega;\ -2 - \omega^2$, wo ω eine imaginäre 3. Einheitswurzel ist.

3. Welches sind die Wurzeln für $d = 7$?

4. Die Diskriminante von $x^3 - 27xy^2 + 54y^3$ ist Null.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

8. Homogeneität der Kovarianten eines Formensystems.

Satz 5: Eine in den Variabeln nichthomogene Kovariante ist eine Summe von (in den Variabeln) homogenen Kovarianten.

Angenommen, die Koeffizienten des Formensystems seien (in irgendwelcher Ordnung) $a, b, \ldots$ K sei eine Kovariante, d. h.

$$K(A, B, \ldots; \xi, \eta; \ldots) = \Delta^{\vartheta} \cdot K(a, b, \ldots; x, y; \ldots).$$

Werden nun $x, y, \ldots$ durch ihre in $\xi, \eta, \ldots$ linearen Ausdrücke ersetzt, so werden die Glieder auf der rechten Seite, welche die Ordnung n_1 haben, — und nur solche Glieder — in ihrer Gesamtheit gleich den Gliedern auf der linken Seite, welche in $\xi, \eta \ldots$ von der Ordnung n_1 sind. Bezeichnet daher K_1 die Summe aller Glieder von K von der Ordnung n_1, so hat man

$$K_1(A, B, \ldots; \xi, \eta, \ldots) = \Delta^{\vartheta} \cdot K_1(a, b, \ldots; x, y, \ldots),$$

so daß K_1 eine Kovariante des Systems darstellt. Ähnlich ist die Summe K_2 aller Glieder aus K von Ordnung n_2 eine solche Kovariante, usw., so daß K eine Summe von lauter in den Variabeln homogenen Kovarianten ist.

Satz 6: Wenn eine Kovariante von 2 oder mehr Formen nicht homogen in den Koeffizienten jeder einzelnen Form ist, so ist sie eine Summe von lauter (in den Koeffizienten jeder einzelnen Form) homogenen Kovarianten.

Der Beweis verläuft vollkommen dem eben geführten parallel. Mit Benutzung der Bezeichnungen von Beispiel 9 in 5. setze man $d = ac - b^2$. Dann ist $s + 3d$ eine Invariante von f und g vom Gewichte 2. Durch eine lineare Transformation mit der Determinante Δ mögen f und g in

$$F = A\xi^2 + 2B\xi\eta + C\eta^2, \quad G = P\xi^2 + 2Q\xi\eta + R\eta^2$$

übergehen, wo A, B, C lineare Funktionen von a, b, c und P, Q, R lineare Funktionen von p, q, r sind. Nach Voraussetzung ist

$$AR - 2BQ + CP + 3(AC - B^2) = \Delta^2(s + 3d).$$

Auf der rechten Seite entspringen die in a, b, c quadratischen Glieder $3d\Delta^2$ nur dem Teil $3(AC - B^2)$ auf der linken Seite. Daher ist d selbst eine quadratische Invariante; ebenso ist s selbst eine Invariante.

Nach Satz 5 und 6 dürfen wir uns daher von jetzt an auf Kovarianten beschränken, die in den Variablen und Koeffizienten jeder einzelnen Form homogen sind.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 7: $f_1, \ldots, f_r$ seien Formen in $x_1, \ldots, x_q$ mit den Ordnungen $p_1, \ldots, p_r$. K sei eine Kovariante dieser Formen von der Ordnung n und dem Gewicht g und sei vom Grade d_i in den Koeffizienten von f_i. Dann besteht zwischeu n, q, g und den p und d die Beziehung

$$\sum p_i d_i = gq + n.$$

f_i habe die Koeffizienten $c_{ik} (k = 1, 2, \ldots)$. Durch die Transformation

$$x_1 = m y_1, \ldots, x_q = m y_q$$

mit der Determinante m^q geht f_i in eine Form mit den Koeffizienten $C_{ik} = m^{p_i} c_{ik}$ über. Dann ist also

$$K(m^{p_1} c_{1k}, \ldots, m^{p_r} c_{rk}; m^{-1} x_1, \ldots, m^{-1} x_q) \equiv (m^q)^g K(c_{1k}, \ldots, c_{rk}; x_1, \ldots, x_q),$$

identisch in $m, x_1, \ldots, x_q, c_{1k}, \ldots, c_{rk}$, wo jedes k seine Werte durchläuft. Links können wir den Faktor m^{-1} entfernen und dafür m^{-n} vor den ganzen Ausdruck setzen. Dann bekommen wir, da K vom Grade d_i in den $c_{ik} (k = 1, 2, \ldots)$ ist,

$$m^{-n} m^{p_1 d_1} \ldots m^{p_r d_r} = m^{qg},$$

womit unser Satz bewiesen ist.

Nehmen wir die Kovariante einer einzelnen Form und greifen aus ihr ein beliebiges Glied heraus. Es möge den Grad d haben. Dann ist nach unserem Satz $pd = n + qg$. Daher ist der Grad d allen Gliedern gemeinsam.

Satz 8: Eine Kovariante konstanter Ordnung n einer einzelnen Form f ist von konstantem Grade in den Koeffizienten von f.

9. Gewicht der Koeffizienten einer Kovariante einer binären Form. Wir benötigen von jetzt an eine andere Bezeichnung für die Koeffizienten einer Form, nämlich

$$(11) \quad f = a_0 x^p + p a_1 x^{p-1} y + \cdots + \binom{p}{i} a_i x^{p-i} y^i + \cdots + a_p y^p,$$

wo die Binomialkoeffizienten p usw. hinzugefügt sind, um später Brüche zu vermeiden. Als Gewicht von a_k definiert man k und als Gewicht eines Produkts von Faktoren a_k die Summe der Gewichte der Faktoren.

Um (6) mit unserer jetzigen Bezeichnung in Übereinstimmung zu bringen, ersetze man a, b, c, d durch a_0, a_1, a_2, a_3. Dann wird die Hessesche Form (7)

$$36(rx^2 + 2sxy + ty^2),$$

$$(12) \quad r = a_0 a_2 - a_1^2, \; 2s = a_0 a_3 - a_1 a_2, \; t = a_1 a_3 - a_2^2.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Glieder von r bzw. s bzw. t haben konstantes Gewicht, nämlich 2 bzw. 3 bzw. 4. Da die Hessesche Form das Gewicht 2 hat, so legt uns dies den Satz nahe:

Satz 9: In einer Kovariante

$$K = \sum_0^n S_r(a)\, x^{n-r} y^r \tag{13}$$

einer einzelnen Form (11) von der Ordnung n und dem Gewicht g haben alle Glieder des Koeffizienten $S_r(a)$ dasselbe Gewicht $g + r$. Insbesondere ist das Gewicht des Leitgliedes $S_0(a)$ der Kovariante gleich dem Gewicht g.

Die Transformation $x = \xi$, $y = m\eta$ ersetzt f durch eine Form mit den Koeffizienten $A_i = m^i a_i$. Nach der Definition einer Kovariante K vom Gewicht g haben wir

$$\sum_{r=0}^{n} S_r(A)\, \xi^{n-r} \eta^r = m^g \sum_{r=0}^{n} S_r(a)\, x^{n-r} y^r. \tag{14}$$

Ein Glied von $S_r(a)$ sei $t = c a_0^{e_0} a_1^{e_1} \ldots a_p^{e_p}$; sein Gewicht ist $\omega_r = e_1 + 2e_2 + \cdots + pe_p$. Die linke Seite von (14) enthält das Glied

$$c A_0^{e_0} A_1^{e_1} \ldots A_p^{e_p} \xi^{n-r} \eta^r = t x^{n-r} y^r m^{\omega_r - r},$$

welches gleich einem Gliede auf der rechten Seite von (14) sein muß. Daraus folgt, daß $\omega_r - r = g$. Damit ist unser Satz bewiesen.

Jedes $S_r(a)$ heißt, da es konstantes Gewicht hat, isobar. Erteilen wir noch x das Gewicht 1 und y das Gewicht Null, so sehen wir, daß jedes Glied von (13) das konstante Gesamtgewicht $g + n$ besitzt.

Folgerung: Ein homogenes Polynom ist dann und nur dann eine Kovariante in bezug auf Transformationen der Gestalt $x = \xi$, $y = m\eta$, wenn es isobar ist.

Übungen: 1. Bestätige Satz 9 für die Kovariante f von f.

2. Für eine Invariante vom Gewicht g und vom Grade d einer binären Form $p$ter Ordnung ist $pd = 2g$.

3. Daher hat keine binäre Form ungrader Ordnung eine Invariante ungraden Grades.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

10. Seminvarianten. Ein in den Koeffizienten einer binären Form f homogenes isobares Polynom heißt eine Seminvariante von f, wenn es sich gegenüber allen Transformationen von der Art

$$T_k : x = \xi + k\eta, \quad y = \eta$$

invariant verhält.

$A_0, A_1, \ldots$, seien die Koeffizienten der durch T_k transformierten Form. Obwohl für unsere Untersuchung unwesentlich, sei doch hier angeführt, daß

$$(15) \qquad A_0 = a_0, \; A_1 = a_1 + k a_0, \; A_2 = a_2 + 2k a_1 + k^2 a_0.$$

Die erste Gleichung erweist a_0 als Seminvariante von f. Die Elimination von k zwischen den beiden letzten Gleichungen ergibt

$$A_0 A_2 - A_1^2 = a_0 a_2 - a_1^2,$$

so daß auch $a_0 a_2 - a_1^2$ eine Seminvariante von f ist. Sie ist das Leitglied der Hesseschen Form von f für $p = 3$, wie schon vor Satz 9 erwähnt wurde. Da auch a_0 ein Leitglied, nämlich das von f selbst, ist, so legen uns diese beiden Fälle den Satz nahe:

Satz 10: Das Leitglied jeder Kovariante K einer binären Form f ist eine Seminvariante von f.

Nach Satz 9 ist das Leitglied $S_0(a)$ jeder Kovariante (13) isobar und nach Satz 8 homogen. Da K eine Kovariante von f gegenüber allen unimodularen Transformationen (d. h. solchen mit der Determinante 1) T_k ist, so haben wir

$$K = \sum S_r(A)\, \xi^{n-r} \eta^r = \sum S_r(A)\, (x - ky)^{n-r} y^r.$$

Ein Vergleich des Koeffizienten von x^n mit dem in (13) ergibt $S_0(a) = S_0(A)$. Daher ist $S_0(a)$ eine Invariante von f gegenüber allen Transformationen T_k, womit unser Satz 10 bewiesen ist.

Gemäß T_k ist $x - ry = \xi - (r - k)y$, so daß bei der Transformation jede Wurzel r_i von $f\left(\frac{x}{y}, 1\right) = 0$ um k vermindert wird. Daher bleibt die Differenz irgend zweier Wurzeln unverändert.

Da nun in (15) $A_1 = 0$ wird, wenn wir $k = -\frac{a_1}{a_0}$ setzen, so ersetzt die zugehörige Transformation T_k f durch die reduzierte Form

$$g = a_0 \cdot \xi^p + \binom{p}{2} b_2 \xi^{p-2} \eta^2 + \binom{p}{3} b_3 \xi^{p-3} \eta^3 + \cdots,$$

wo $$b_2 = a_2 - \frac{a_1^2}{a_0}, \quad b_3 = a_3 - 3\frac{a_1 a_2}{a_0} + 2\frac{a_1^3}{a_0^2}, \ldots.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Wurzeln von $g = 0$ sind

$$r_i + \frac{a_1}{a_0} = [(r_i - r_1) + \cdots + (r_i - r_p)] : p \qquad (i = 1, \ldots, p).$$

Daher ist jede Wurzel von $g = 0$ eine lineare Funktion der Wurzeldifferenzen von $f = 0$ und bleibt daher bei jeder Transformation T_k ungeändert. Letzteres ist also auch der Fall für $\frac{b_2}{a_0}, \frac{b_3}{a_0}, \ldots$, da diese gleich numerischen Vielfachen der elementarsymmetrischen Funktionen der Wurzeln von $g = 0$ sind. Daher sind auch die homogenen isobaren Polynome

$$(16) \qquad \begin{cases} S_2 = a_0 b_2 \ = a_0 a_2 \ - a_1^2, \\ S_3 = a_0^2 b_3 = a_0^2 a_3 - 3 a_0 a_1 a_2 \ + 2 a_1^3, \\ S_4 = a_0^3 b_4 = a_0^3 a_4 - 4 a_0^2 a_1 a_3 + 6 a_0 a_1^2 a_2 - 3 a_1^4, \\ \text{usw. bis } S_p \end{cases}$$

Invarianten von f gegenüber allen Transformationen T_k, d. h. es sind Seminvarianten von f.

Da g aus f durch eine unimodulare lineare Transformation abgeleitet wurde, so hat jede Seminvariante S von f die Eigenschaft

$$S(a_0, \ldots, a_p) = S(a_0, \ 0, \ b_2, \ldots, b_p) = S\left(a_0, \ 0, \ \frac{S_2}{a_0}, \ldots, \frac{S_p}{a_0^{p-1}}\right).$$

Daraus folgt

Satz 11: Jede Seminvariante von f ist der Quotient eines Polynoms in den Seminvarianten $a_0, S_2, \ldots, S_p$ und einer Potenz von a_0.

Wir werden diesen Satz sogleich anwenden, um alle Seminvarianten für $p < 5$ zu finden. Aus Satz 10 wissen wir schon, daß sich unter ihnen die Leitglieder aller Kovarianten befinden.

Unsere nächste Aufgabe wird dann darin bestehen, alle Kovarianten K mit gegebenem Leitglied zu finden. Als Vorbereitung dazu beweisen wir den

Satz 12: Wenn S eine Seminvariante vom Grade d und Gewicht w einer binären Form f von der Ordnung p ist, so hat jede Kovariante K von f mit dem Leitgliede S die Ordnung $n = pd - 2w$, und es existiert höchstens eine solche Kovariante.[1])

Nach Satz 9 ist das Gewicht von S gleich dem Gewicht g von K. Nach Satz 7 haben wir für $r = 1$, $q = 2$ die Gleichung $pd - n = 2g$,

1) Daß wirklich ein solches K immer existiert, wird in 16. bewiesen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

woraus sich ergibt, daß die Ordnung n von K eindeutig durch S bestimmt ist.

Wenn zwei verschiedene Kovarianten $Sx^n + \cdots$ von f existieren, so haben sie, wie wir eben bewiesen, dasselbe Gewicht $g = w$, so daß ihre Differenz eine Kovariante von f mit dem Faktor y, also von der Form $y \cdot q(a_0, \ldots, a_q; x, y)$ ist. Man wähle zwei voneinander unabhängige lineare Funktionen ξ und η von x und y. Mit Rücksicht auf die Transformation mit der Determinante Δ, welche x und y linear durch ξ und η ausdrückt, haben wir

$$\eta \cdot q(A_0, \ldots, A_p; \xi, \eta) = \Delta^g \cdot y \cdot q(a_0, \ldots, a_p; x, y).$$

Daher ist yq von der Ordnung n und hat den ganz willkürlichen Faktor η. Da wir also durch unsere Annahme auf einen offenbaren Widerspruch gestoßen sind, so ist Satz 12 vollständig bewiesen.

Folgerung: Das Gewicht einer Invariante vom Grade d einer binären Form $p$ter Ordnung ist $\frac{1}{2}pd$.

11. *Satz 13: Jede binäre lineare Transformation ist ein Produkt von Transformationen der 3 Typen*

$$\begin{aligned} T_n &: x = \xi + n\eta, \quad y = \eta \\ S_m &: x = \xi, \quad y = m\eta \qquad (m \neq 0) \\ V &: x = -\eta, \quad y = \xi. \end{aligned}$$

Aus ihnen erhalten wir $V^3 = V^{-1} : x = \eta, y = -\xi$ und

$$\begin{aligned} R_n = V^{-1} T_{-n} V &: x = X, \quad y = Y + nX \\ P_m = V^{-1} S_m V &: x = mX, \quad y = Y \qquad (m \neq 0). \end{aligned}$$

Dann läßt sich die Transformation $x = a\xi + b\eta$, $y = c\xi + d\eta$, $D = ad - bc \neq 0$ darstellen durch

$$S_d P_{\frac{D}{d}} T_{\frac{bd}{D}} R_{\frac{c}{d}}, \text{ wenn } d \neq 0,$$

oder durch $$S_c P_{-b} T_{-\frac{a}{b}} V, \text{ wenn } d = 0.$$

Durch Anwendung der Folgerung aus Satz 9 und unter Berücksichtigung der Wirkung, welche die unimodulare Transformation V hat, erhalten wir die

Folgerung: Ein Polynom in $a_0, \ldots, a_q, x, y$, welches homogen in x und y ist, ist dann und nur dann eine Kovariante der Form (11) wenn es isobar ist, sich kovariant gegenüber allen T_n verhält und

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

ungeändert bleibt, wenn x durch y, y durch $-x$ und a_i durch $(-1)^i a_{p-i}$ $(i = 0, 1, \ldots, p)$ ersetzt wird. Daher ist auch eine Seminvariante, die durch die letzten Vertauschungen ungeändert bleibt, eine Invariante.

12. Das vollständige System von Kovarianten einer binären Form $p$ter Ordnung für $p < 5$. Wir werden eine endliche Zahl von ganzen rationalen Kovarianten $K_1, K_2, \ldots, K_n$ der binären Form f $p$ter Ordnung aufstellen, so daß jede ganze rationale Kovariante von f als Polynom in $K_1, \ldots, K_n$ mit numerischen Koeffizienten darstellbar ist. Man sagt, daß diese $K_1, \ldots K_n$ ein vollständiges System von Kovarianten von f bilden.

Wir werden dazu zunächst ein vollständiges System von Seminvarianten $s_1, s_2, \ldots$ von f aufstellen, so daß also jede andere Seminvariante von f ein Polynom von diesen ist. Wir werden sie als die Leitglieder bekannter Kovarianten $K_1, K_2, \ldots$ von f erkennen. Nun hat jede Kovariante K von f als Leitglied eine Seminvariante, die naturgemäß ein Polynom $P(s_1, s_2, \ldots)$ unserer Elemente des Systems ist. Alle Glieder $cs_1^a s_2^b \ldots$ von P haben dasselbe Gewicht $aw_1 + bw_2 + \cdots$ (wenn w_i das Gewicht von s_i bedeutet). Nun ist aber nach Satz 9 $cK_1^a K_2^b \ldots$ eine Kovariante vom Gewicht $aw_1 + bw_2 + \cdots$, und da alle Glieder von $P(K_1, K_2, \ldots)$ dasselbe Gewicht haben, so ist P eine Kovariante von f. Da es andererseits dasselbe Leitglied wie K hat, so ist es nach Satz 12 mit K identisch. Unser Problem ist also gelöst, wenn wir für die Seminvarianten ein vollständiges System angeben.

Für $p = 1$ zeigt Satz 11, daß jede Seminvariante von $f = a_0 x + a_1 y$ ein Polynom in a_0 ist. Da a_0 das Leitglied von f ist, so haben wir

Satz 14: Jede ganze rationale Kovariante von $f = a_0 x + a_1 y$ ist ein Polynom in f, so daß f selbst das vollständige System von Kovarianten von f darstellt.

Für $p = 2$ zeigt Satz 11, daß jede Seminvariante der Quotient eines Polynoms $P(a_0, S_2)$ und a_0^e ist. Da nun S_2 nicht durch a_0 teilbar ist, so ist P nur dann durch a_0 teilbar, wenn alle seine Glieder explizite den Faktor a_0 haben. Streicht man den Faktor a_0 in P und a_0^e, so reduziert sich das Problem auf das gleiche, nur daß jetzt $e - 1$ an Stelle von e steht, und so kann man fortfahren, bis $e = 0$ ist. Daher ist jede Seminvariante ein Polynom in a_0 und S_2. Da nun a_0 das Leitglied von f, während S_2 nach 4. eine Invariante von f ist, so haben wir

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Satz 15: Jede ganze rationale Kovariante der binären quadratischen Form f ist ein Polynom in f und ihrer Diskriminante S_2.

Für $p > 2$ ist ein anderes Verfahren nötig, da hier Seminvarianten existieren, die keine Polynome in a_0 und den S_i sind. Für die von a_0 freien Glieder von S_i schreibe man Σ_i, so daß z. B. nach (16)

$$\Sigma_2 = -a_1^2; \quad \Sigma_3 = 2a_1^3; \quad \Sigma_4 = -3a_1^4. \tag{17}$$

Für $p = 3$ ist $4\Sigma_2^3 + \Sigma_3^2 = 0$. Also muß $4S_2^3 + S_3^2$ den Faktor a_0 haben. Man findet, daß

$$4S_2^3 + S_3^2 \equiv a_0^2 \cdot D, \tag{18}$$

wo nach (10) und (12)

$$D = a_0^2 a_3^2 - 6a_0 a_1 a_2 a_3 + 4a_0 a_2^3 + 4a_1^3 a_3 - 3a_1^2 a_2^2 \tag{19}$$

die Diskriminante der kubischen Form f ist. Vermittels (18) können wir die zweiten und höheren Potenzen von S_3 aus jedem Polynom in a_0, S_2, S_3 eliminieren und nach Satz 11 schließen, daß jede Seminvariante von der Form $\frac{P}{a_0^e}$ ist, wo P ein Polynom in a_0, S_2, S_3, D ist, welches S_3 in höchstens erstem Grade enthält. Für $e = 0$ ist P von selbst eine Seminvariante. Es sei daher $e \geqq 1$. Sollte jedes Glied von P explizite den Faktor a_0 haben, so spalten wir ihn von P und a_0^e ab und führen dadurch das Problem auf das ähnliche zurück, wo $e - 1$ an Stelle von e steht. Es bleibt so nur der Fall zu behandeln, wo nicht jedes Glied von P den expliziten Faktor a_0 besitzt. Dann ist aber P, durch a_0, a_1, a_2, a_3 ausgedrückt überhaupt nicht a_0 teilbar, d. h. P hat auch nicht implizite den Faktor a_0, denn sonst wäre

$$P_1 \equiv P(0, \Sigma_2, \Sigma_3, d) \equiv 0, \quad \text{wo} \quad d = 4a_1^3 a_3 - 3a_1^2 a_2^2.$$

Da aber a_3 in d, jedoch nicht in Σ_2 oder Σ_3 vorkommt, so muß P_1 frei von d sein. Ferner kann die erste Potenz von $\Sigma_3 = 2a_1^3$ durch kein Polynom in $\Sigma_2 = -a_1^2$ aufgehoben werden, so daß P_1 auch frei von Σ_3 und endlich von Σ_2 ist.

Daher ist jede Seminvariante der kubischen Form f ein Polynom in a_0, S_2, S_3, D. Sie sind miteinander verbunden durch die Syzygie (18), d. h. durch eine Beziehung, die keine der 4 Größen ganz und rational durch die 3 anderen ausdrückt.

Satz 16: Das vollständige System der ganzen und rationalen Kovarianten der binären kubischen Form f besteht aus f, der Diskri-

Digitized by Google Original from UNIVERSITY OF MICHIGAN

minante D, der Hesseschen Form $36H$ und der Funktionaldeterminante $3G$ von f und H. Sie sind durch die Cayleysche Syzygie

$$4H^3 + G^2 \equiv f^2 \cdot D \tag{20}$$

miteinander verbunden.

Dies folgt daraus, daß a_0, S_2, S_3 die Leitglieder der Kovarianten f, H, G sind. —

Betrachten wir jetzt den Fall $p = 4$. Aus (17) sehen wir, daß die einfachste Beziehung $3\Sigma_2^2 + \Sigma_4 = 0$ ist. Daher ist $3S_2^2 + S_4$ durch a_0 teilbar, und wir finden, daß

$$S_4 + 3S_2^2 \equiv a_0^2 \cdot I, \quad \text{wo} \quad I = a_0 a_4 - 4a_1 a_3 + 3a_2^2.$$

Diese Identität benutzen wir, um S_4 auszuschalten und betrachten jetzt Polynome $P(a_0, S_2, S_3, I)$, welche wie dasjenige in (18) a_0 implizit, aber nicht explizit als Faktor enthalten. Für $a_0 = 0$ wird $D = -a_1^2 \cdot I = \Sigma_2 \cdot I$. Infolgedessen besitzt $D - S_2 \cdot I$ den Faktor a_0, und durch Ausrechnen findet man, daß

$$S_2 \cdot I - D \equiv a_0 \cdot J,$$

wo
$$J = a_0 a_2 a_4 - a_0 a_3^2 + 2a_1 a_2 a_3 - a_1^2 a_4 - a_2^3.$$

Die Elimination von D zwischen dieser Identität und (18) führt auf die Gleichung

$$a_0^3 J - a_0^2 S_2 I + 4S_2^3 + S_3^2 = 0, \tag{21}$$

welche uns in den Stand setzt, die zweiten und höheren Potenzen von S_3 aus P zu eliminieren und so ein Polynom Q in a_0, S_2, S_3, I, J zu erhalten, welches in S_3 von höchstens erstem Grade ist. An genommen, es sei möglich, daß Q implizite, aber nicht explizite den Faktor a_0 enthielte. Dann wäre

$$Q(0, -a_1^2, 2a_1^3, 3a_2^2 - 4a_1 a_3, J) \equiv 0$$

Mit Rücksicht auf die in J vorkommende Größe a_4 könnte J überhaupt nicht in Q vorkommen, und aus ähnlichen Gründen nicht I. Auch könnte Q wegen der ungraden Potenz a_1^3 nicht die erste Potenz von S_3 enthalten, müßte also ganz frei von S_3 und daher auch von S_2 sein.

Daher ist jede Seminvariante der biquadratischen Form f eine ganze rationale Funktion von a_0, S_2, S_3, I, J. Letztere sind durch die Syzygie (21) miteinander verbunden.

Bezeichnet man die Hessesche Kovariante von f mit $144\,H$, die Jacobische Kovariante von f und H mit $8\,G$, so sind a_0, S_2 und S_3 die Leitglieder von f, H und G. Nach der Folgerung in 11.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

sind die Seminvarianten I und J Invarianten von f, da sie ungeändert bleiben, wenn wir a_0 mit a_4 und a_1 mit $-a_3$ vertauschen.

Satz 17: Das vollständige System ganzer rationaler Kovarianten der binären biquadratischen Form f besteht aus f, den Invarianten I und J, der Hesseschen Form 144 H *und der Funktionaldeterminante* 8 G *von f und H. Zwischen ihnen besteht die Syzygie*

$$f^3 J - f^2 H I + 4H^3 + G^2 \equiv 0. \tag{22}$$

13. Kanonische Form der binären biquadratischen Form. Lösung der biquadratischen Gleichung. Scheiden wir den uninteressanten Fall, bei dem $f\left(\frac{x}{y}, 1\right) = 0$ mehrfache Wurzeln hat, aus, so ist $f(x, y)$ das Produkt von vier Linearformen, von denen keine zwei zueinander proportionale Koeffizienten haben. Führt man zwei von ihnen als neue Variabeln ξ und η ein, so läßt sich f durch eine lineare Transformation auf die Form $\xi\eta q$ bringen, wo

$$q = g\xi^2 + 2h\xi\eta + k\eta^2$$

ist. Da weder ξ noch η ein Faktor von q ist, so ist $gk \neq 0$, und man kann r, s, t so wählen, daß

$$t^2 = \frac{k}{g}, \quad r + s = g, \quad r - s = \frac{h}{t}.$$

Dann ist
$$\xi\eta = \tfrac{1}{4}t^{-1}[(\xi + t\eta)^2 - (\xi - t\eta)^2],$$
$$q = r(\xi + t\eta)^2 + s(\xi - t\eta)^2.$$

Nach Einführung der neuen Variablen

$$X = \sqrt[4]{\frac{r}{4t}}(\xi + t\eta), \quad Y = \sqrt[4]{-\frac{s}{4t}}(\xi - t\eta)$$

nimmt jetzt $f = \xi\eta q$ die kanonische Form

$$X^4 + Y^4 + 6mX^2Y^2 \tag{23}$$

an. Daß hier noch ein Parameter m auftritt, erklärt sich durch die Existenz der rationalen absoluten Invariante $\frac{I^3}{J^2}$ — d. h. einer Invariante vom Gewichte Null —, die daher für f und für alle Formen, welche wie (23) aus f durch lineare Transformation hervorgehen, denselben Wert hat. — Bei den kubischen Formen ohne mehrfache Wurzeln trat in der kanonischen Form kein Parameter mehr auf, sie alle waren auf die Gestalt $X^3 + Y^3$ transformierbar. Jede nichtsinguläre kubische Form ließ sich daher auch in jede andere nichtsinguläre Form überführen. Anders

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ist es, wie wir sehen, bei den (nichtsingulären) biquadratischen Formen, sie lassen sich nicht ohne weiteres ineinander transformieren, vielmehr ist dazu die Gleichheit der absoluten Invariante $\frac{I^3}{J^2}$ oder — was auf dasselbe hinauskommt — die Gleichheit von m erforderlich.

Damit haben wir bewiesen, daß jede biquadratische Form sich auf die kanonische Form (23) bringen läßt. Zu diesem Beweis mußten wir allerdings die Wurzeln von $f\left(\frac{x}{y}, 1\right) = 0$ kennen. Weiß man aber, daß eine solche kanonische Form existiert, so kann man auch ohne Kenntnis der Wurzeln diese Form herstellen und dies, wie Cayley gezeigt hat, dazu benutzen, um umgekehrt nun die *Wurzeln* zu berechnen: Wir können, wie wir wissen, f immer auf die Gestalt (23) bringen, und umgekehrt. Letztere Transformation habe die Determinante Δ. Die Invarianten I und J von (23) sind, da $a_0 = a_4 = 1$, $a_1 = a_3 = 0$, $a_2 = m$, gleich $1 + 3m^2$ bzw. $m - m^3$. Da sie das Gewicht 4 bzw. 6 haben, so ist also

$$f = X^4 + Y^4 + 6mX^2Y^2,$$

$$I = \Delta^4(1 + 3m^2), \quad J = \Delta^6(m - m^3),$$

wo sich I und J auf f beziehen. Es handelt sich, wenn wir die kanonische Form herstellen wollen, darum, X, Y und m zu bestimmen. Nun besteht für $\Delta^2 m$ die Gleichung

$$4(\Delta^2 m)^3 - I(\Delta^2 m) + J = 0. \tag{24}$$

Berechnet man hieraus $\Delta^2 m$ und aus $\Delta^4 = I - 3(\Delta^2 m)^2$ die Größe Δ^2 — mit beliebigem Vorzeichen der Quadratwurzel genommen — so ergibt sich m. — Um jetzt noch die Größen X und Y zu finden, berechnen wir die Hessesche Form von (23). Sie ist

$$144 \begin{vmatrix} X^2 + mY^2 & 2mXY \\ 2mXY & Y^2 + mX^2 \end{vmatrix}.$$

Bezeichnet man die Hessesche Form von f mit $144H$, so ist

$$H = \Delta^2\{m(X^4 + Y^4) + (1 - 3m^2)X^2Y^2\}.$$

Eliminiert man $X^4 + Y^4$ aus f und H, so erhält man

$$\Delta^2 mf - H = \Delta^2(9m^2 - 1)X^2Y^2.$$

Hieraus läßt sich XY berechnen, denn die linke Seite ist ein vollständiges Quadrat und von Null verschieden. Denn wenn $9m^2 = 1$ wäre, so wäre f das Quadrat von $X^2 \pm Y^2$ und hätte

Digitized by Google Original from UNIVERSITY OF MICHIGAN

entgegen unserer Voraussetzung eine mehrfache Wurzel. Aus XY und f erhält man nun der Reihe nach $X^2 + Y^2$, $X + Y$, $X - Y$ und so endlich X und Y.

Satz 18: Jede binäre biquadratische Form $f(x, y)$, die nicht durch das Quadrat einer linearen Form teilbar ist, läßt sich auf die kanonische Form (23) bringen. Dazu ist die Lösung einer kubischen Gleichung und das Ziehen einer Quadratwurzel notwendig.

Die nun entstandene Gleichung $X^4 + Y^4 + 6mX^2Y^2 = 0$ läßt sich aber leicht in Linearfaktoren zerlegen, wenn man $\frac{X^2}{Y^2} = z$ setzt.

Satz 19: Um also eine biquadratische Gleichung $q(w) = 0$, die keine mehrfache Wurzel hat, zu lösen, bringe man die Form $f(x, y) = y^4 q\left(\frac{x}{y}\right)$ auf ihre kanonische Form (23) und zerlege sie in Linearfaktoren. Die kubische Hilfsgleichung (24) wird nach 7. aufgelöst. Zur Lösung einer biquadratischen Gleichung ist daher das Ziehen einer dritten und mehrerer Quadratwurzeln notwendig.

Betr. Tafeln von Invarianten und Kovarianten vergleiche man Faà di Bruno, Theorie der binären Formen, Leipzig 1881.

Übungen: 1. Für $I = 0$ und $\Delta \neq 0$ ist $3m^2 = -1$. Man zeige, daß für die Gleichung $w^4 - Sw^2 - \frac{3}{4}Tw - \frac{1}{12}S^2 = 0$, welche in der Theorie der Wendepunkte einer ebenen Kurve dritter Ordnung eine wichtige Rolle spielt, $I = 0$, und finde ihre quadratischen Faktoren.

2. Man finde die drei kanonischen Formen, wenn $J = 0$. Das Resultat wende man auf die Lösung der Gleichung $w^4 + cw^3 \pm cw - 1 = 0$ an.

Geometrische Anwendungen der Invariantentheorie. Wir wollen noch in aller Kürze das auf die Geometrie Bezügliche der vorhergehenden Theorie besprechen. — Die Variabeln $x_1, x_2, \ldots, x_n$ deuten wir als homogene Koordinaten eines Punktes im Raum von der Stufe n (d. h. der Dimension $n - 1$), so daß ein Punkt mit den Koordinaten $kx_1, kx_2, \ldots, kx_n$, wo k ein numerischer Faktor ist, mit dem vorigen Punkt übereinstimmt. Man schreibt deshalb die Koordinaten in der Form $x_1 : x_2 : x \ldots : x_n$. Eine Form f $m$ter Ordnung gleich Null gesetzt liefert dann eine „Fläche" $m$ter Ordnung im R_{n-1}. Einer linearen Transformation der homogenen Variabeln entspricht eine projektive Transformation des R_{n-1}. Bei dieser Transformation bleibt trotz vieler Veränderungen manches im Raum erhalten, z. B. die Ordnungszahl einer Fläche, so daß aus einer Fläche $m$ter Ordnung wieder eine solche hervorgeht. Ebenso bleibt die Klasse einer Fläche erhalten. Ordnungs- und Klassenzahl einer Fläche sind also projektive numerische Invarianten. — Nun ist für eine Fläche aber

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

nicht nur ihre Ordnung oder Klasse charakteristisch, sondern auch das Verschwinden bzw. Nichtverschwinden gewisser aus den Koeffizienten ihrer Gleichung gebildeter Ausdrücke, d. h. solcher Ausdrücke, die für die transformierte Fläche auch verschwinden bzw. nicht verschwinden, die sich also bei einer solchen projektiven Transformation nur mit einem Faktor reproduzieren, der von der Transformation abhängt. Eine genauere Untersuchung zeigt, daß dieser Faktor nur eine Potenz der Transformationsdeterminante sein kann. Damit sind wir bei Bekanntem angelangt: Für die Fläche ist das Verschwinden bzw. Nichtverschwinden von Invarianten charakteristisch. Und umgekehrt hat jede solche Invariante eine geometrische Bedeutung. Ist z. B. f eine ternäre quadratische Form, so bilden die Punkte, die die Gleichung $f = 0$ befriedigen, einen Kegelschnitt. Bei projektiver Transformation geht aus ihm wieder ein Kegelschnitt hervor. Nun besitzt aber eine ternäre quadratische Form eine Invariante: die Hessesche Determinante. Der Kegelschnitt hat nun ganz verschiedene Gestalt, je nachdem diese Invariante für ihn verschwindet oder nicht. Im letzteren Fall ist er eine Ellipse, Hyperbel, Parabel oder ein Kreis. Er heißt dann nichtzerfallend oder irreduzibel. Im ersteren Fall zerfällt er in ein Geradenpaar, er heißt reduzibel. Alle irreduziblen Kegelschnitte sind untereinander äquivalent, d. h. sie können durch eine projektive Transformation ineinander übergeführt werden. — Gehen wir zum binären Gebiet über, so liefert eine Form $n$ter Ordnung gleich Null gesetzt eine Gesamtheit von n Punkten. Sind diese n Punkte alle voneinander verschieden, so ist die Diskriminante der Form von Null verschieden. Verschwindet aber diese Invariante, so fallen mehrere der Punkte zusammen, und dieses Zusammenfallen läßt sich natürlich durch keine Transformation aufheben, es ist also eine projektive Eigenschaft. Fallen insbesondere alle Punkte zusammen, so ist die Form eine reine Potenz. — Aus 12. wissen wir, daß eine quadratische und kubische Form nur diese eine Invariante, ihre Diskriminante, hat, daß eine biquadratische Form aber außerdem noch eine Invariante, nämlich I oder J, besitzt (I oder J deshalb, weil die Diskriminante, I und J voneinander abhängig sind). $J = 0$ bedeutet z. B., daß die durch die Gleichung dargestellten Punkte in harmonischer Lage liegen; und diese Eigenschaft kann ja bekanntlich durch keine projektive Transformation aufgehoben werden. — Die Begründer der Invariantentheorie glaubten nun anfangs, daß die Invarianten alle geometrischen Eigenschaften der Kurve oder Fläche wiedergäben, bis schließlich Aronhold erkannte, daß für eine

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Fläche auch gewisse andere Ausdrücke, und zwar solche, die auch noch Variabeln enthalten, charakteristisch seien. Hier kam es jetzt natürlich darauf an, ob solche Ausdrücke identisch verschwänden oder nicht. Diese Formen reproduzieren sich bei linearer Transformation wiederum mit einer Potenz der Transformationsdeterminante, es sind die uns bekannten Kovarianten. — So hat z. B. ein Kegelschnitt eine Kovariante, nämlich die Form, die gleich Null gesetzt die Tangente in einem seiner Punkte angibt. Verschwindet diese Form, für einen seiner Punkte gebildet, identisch, so bedeutet auch dies eine besondere geometrische Eigenschaft. Denn da die Tangente dann unbestimmt wird, also jede Gerade durch diesen Punkt eine Tangente ist, d. h. den Kegelschnitt in zwei zusammenfallenden Punkten trifft, so ist dieser Punkt ein Doppelpunkt. Der Kegelschnitt zerfällt also. — Verschwindet für eine Fläche zweiter Ordnung die entsprechende Kovariante, so wird hier die Tangentialebene unbestimmt, die Fläche hat in diesem Punkt eine Spitze, sie ist ein Kegel. — Bei binären Formen, mit denen wir uns ja hauptsächlich beschäftigen, hatten wir die Jacobische Form zweier Formen, insbesondere quadratischer Formen, kennengelernt. Verschwindet diese identisch, so liegen die beiden durch die Formen dargestellten Punktepaare in harmonischer Lage.

Zusammengefaßt: Geometrische Eigenschaften gegenüber projektiven Transformationen, d. h. Eigenschaften, die bei solchen Transformationen erhalten bleiben, werden durch projektive Invarianten und Kovarianten — besser gesagt durch deren Verschwinden bzw. Nichtverschwinden — dargestellt. (Es braucht wohl nicht hinzugefügt zu werden, daß die lineare, d. h. projektive, Transformation nichtsingulär sein muß.)

Es ist daher eine der Hauptaufgaben der Geometrie, für jede Gemeinschaft von Flächen (im allgemeinen Sinn) alle Invarianten und Kovarianten anzugeben und deren Verschwinden geometrisch zu deuten. Diese Aufgabe ist aber bisher nur in den einfachsten Fällen gelöst. — Auf diese Dinge näher einzugehen, verbietet der Raum. Der interessierte Leser wird in den Arbeiten der Geometer, die gegen Ende des vorigen Jahrhunderts lebten, über diese Dinge genügend finden, insbesondere in denen von Aronhold, Cayley, Hesse, Clebsch, Gordan sowie Study, desgleichen in den Lehrbüchern von Study (Einführung in die Theorie der Invarianten, Braunschweig 1923) und Clebsch-Lindemann, Vorlesungen über Geometrie (1. und 2. Auflage, Leipzig).

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

ZWEITES KAPITEL.

FORTFÜHRUNG DER THEORIE DER KOVARIANTEN BINÄRER FORMEN.

Wir werden hier einige grundlegende Sätze über Invarianten und Kovarianten beweisen, welche im einleitenden Kapitel nur für Formen bis zur vierten Ordnung bestätigt wurden, z. B. den Satz, daß alle Kovarianten ganz und rational durch eine endliche Zahl von ihnen ausdrückbar sind. — Für eingehenderes Studium geben wir am Ende des Kapitels einige Anweisungen.

14. Annihilatoren von Kovarianten. Wir gehen aus von der binären Form

$$f = \sum_{i=0}^{p} \binom{p}{i} a_i x^{p-i} y^i \tag{1}$$

(vgl. 9.). Wir wollen sehen, ob zwischen dem Koeffizienten einer Kovariante Beziehungen bestehen. Dazu müssen wir zuerst offenbar Beziehungen zwischen den Koeffizienten A_i der transformierten Form aufsuchen. Wir betrachten nun nicht die allgemeine Transformation, sondern die unimodulare

$$T_n : x = \xi + n\eta, \quad y = \eta.$$

Beziehungen, die bei der allgemeinen Transformation gelten, gelten sicher bei dieser speziellen. Nun laute die transformierte Form

$$f = \sum_{i=0}^{p} \binom{p}{i} A_i \xi^{p-i} \eta^i. \tag{2}$$

Die A_i sind Polynome in $n, a_0, \ldots, a_p$, die wir nicht genauer zu kennen brauchen, denn wir wollen ja nur Beziehungen der A untereinander feststellen. Dazu ist das Hilfsmittel der Differentiation ja oft zweckmäßig. Differenzieren wir (2) nach n, so folgt

$$0 = \sum_{i=0}^{p} \binom{p}{i} \left\{ \frac{\partial A_i}{\partial n} \xi^{p-i} \eta^i - A_i (p-i) \xi^{p-i-1} \eta^{i+1} \right\},$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

da $\eta = y$ von n frei, während $\xi = x - n\eta$ ist. Da dies identisch verschwindet, so muß auch der Koeffizient von $\xi^{p-j}\eta^j$

$$\binom{p}{j}\frac{\partial A_j}{\partial n} - \binom{p}{j-1}(p-j+1)A_{j-1}$$

verschwinden (hier fällt für $j = 0$ das zweite Glied weg). Wegen

$$\binom{p}{j} = \binom{p}{j-1}\cdot\frac{p-j+1}{j}$$

erhalten wir hieraus

$$\frac{\partial A_0}{\partial n} = 0, \quad \frac{\partial A_j}{\partial n} = jA_{j-1} \qquad (j = 1, \ldots, p). \tag{3}$$

Damit haben wir die Beziehungen zwischen den A und n. Suchen wir jetzt die Beziehungen zwischen den Koeffizienten einer Kovariante $K(a_0, \ldots, a_p; x, y)$ und setzen zur Abkürzung

$$k \equiv K(a_0, \ldots, a_p; x, y), \quad K \equiv K(A_0, \ldots, A_p; \xi, \eta),$$

so muß, damit k eine Kovariante gegenüber T_n ist, $K = k$ eine Identität in $n, a_0, \ldots, a_p, x, y$ werden, wenn ξ durch $x - ny$, η durch y und jedes A_i durch seinen Ausdruck in $n, a_0, \ldots, a_p$ ersetzt wird. Da nun k frei von n ist, so folgt aus $k = K$, daß

$$\frac{\partial K}{\partial n} \equiv 0.$$

Umgekehrt folgt aus letzterem, daß K von n unabhängig und daher gleich dem Werte von k ist, auf den es sich für $n = 0$ reduziert. Nun ist

$$\frac{\partial K}{\partial n} = \sum_{j=0}^{p}\frac{\partial K}{\partial A_j}\cdot\frac{\partial A_j}{\partial n} + \frac{\partial K}{\partial \xi}\cdot\frac{\partial \xi}{\partial n} = \sum_{j=1}^{p} jA_{j-1}\cdot\frac{\partial K}{\partial A_j} - \eta\cdot\frac{\partial K}{\partial \xi}. \tag{4}$$

Da dies für alle n identisch verschwinden soll, so muß es insbesondere für $n = 0$ verschwinden, d. h. es muß

$$\Omega k - y\cdot\frac{\partial k}{\partial x} \equiv 0, \quad \text{wobei} \quad \Omega = \sum_{j=1}^{p} ja_{j-1}\frac{\partial}{\partial a_j}. \tag{5}$$

(Identisch für alle $x, y, a_0, \ldots, a_p$). Diese Identität bleibt aber bestehen, wenn wir $x, \ldots, a_p$ durch irgendwelche anderen Größen, etwa durch $\xi, \eta, A_0, \ldots, A_p$ ersetzen, so daß (4) auch in diesen Größen identisch verschwindet. Infolgedessen ist das Bestehen von (5) notwendig und hinreichend dafür, daß K eine Kovariante

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

gegenüber allen Transformationen T_n ist. Wir werden dann sagen, daß k durch den Differentialoperator oder den Annihilator

$$\Omega - y\frac{\partial}{\partial x}\left(\Omega = a_0\frac{\partial}{\partial a_1} + \cdots + p\,a_{p-1}\frac{\partial}{\partial a_p}\right) \tag{6}$$

zum Verschwinden gebracht wird.

Die Form (1) ändert sich nicht, wenn wir x und y, sowie a_i und $a_{p-i}(i = 0, 1, \ldots, p)$ vertauschen. Daher ist k dann und nur dann eine Kovariante gegenüber jeder Transformation

$$R_n : x = \xi, \quad y = \eta + n\xi,$$

wenn es durch den Operator

$$O - x\frac{\partial}{\partial y}\left(O = p\,a_1\frac{\partial}{\partial a_0} + \cdots + (p-i)\,a_{i+1}\frac{\partial}{\partial a_i} + \cdots + a_p\frac{\partial}{\partial a_{p-1}}\right) \tag{7}$$

zum Verschwinden gebracht wird.

Damit endlich k eine Kovariante gegenüber jeder Transformation $S_m: x = \xi$, $y = m\eta$ ist, ist nach 9. Folgerung notwendig und hinreichend, daß es isobar ist. Da nun $T_{-1}R_1T_{-1} = V$, d. h. $x = -Y$, $y = X$ ist, so folgt aus 11. daß jede binäre Transformation durch T_n, R_n, S_m erzeugt werden kann.

Satz 1: Ein Polynom $K(a_0, \ldots, a_p; x, y)$ ist dann und nur dann eine Kovariante der binären Form (1), wenn es isobar ist und durch die beiden Operatoren (6) und (7)[1] zum Verschwinden gebracht wird.

Damit ist der gewünschte Zusammenhang gefunden.

Folgerung 1: Ein Polynom in $a_0, \ldots, a_p$ ist dann und nur dann eine Invariante von (1), wenn es isobar ist und durch Anwendung der Operatoren Ω und O verschwindet.

Z. B. ist nach der Folgerung in 10. das Gewicht einer quadratischen Invariante I von $a_0x^2 + 2a_1xy + a_2y^2$ gleich 2, so daß $I = ra_0a_2 + sa_1^2$ sein muß. Dann ist $\Omega I = 2(r+s)a_0a_1 \equiv 0$, $OI = 2(r+s)a_1a_2 \equiv 0$. Jede dieser Bedingungen ergibt $s = -r$ und daher $I = r(a_0a_2 - a_1^2)$.

Gemäß der Definition einer Seminvariante in 10. haben wir

Folgerung 2: Ein homogenes isobares Polynom in $a_0, \ldots, a_p$ ist dann und nur dann eine Seminvariante von (1), wenn es durch Ω zum Verschwinden gebracht wird.

---

1) Bei Berechnungen ist es zweckmäßiger, nur den Operator (6) zu verwenden. — Wir wenden hier die Folgerung von 11. an.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

15. **Kommutatoren.** Man schreibe jeden der Annihilatoren Ω und O in den folgenden beiden Formen:

$$\Omega = \sum_{j=1}^{p} j a_{j-1} \frac{\partial}{\partial a_j} = \sum_{k=0}^{p-1} (k+1) a_k \frac{\partial}{\partial a_{k+1}},$$

$$O = \sum_{j=1}^{p} (p-j+1) a_j \frac{\partial}{\partial a_{j-1}} = \sum_{k=0}^{p-1} (p-k) a_{k+1} \frac{\partial}{\partial a_k}.$$

Dann ist

$$\Omega O = \sum_{j=1}^{p} j a_{j-1} \Big[(p-j+1) \frac{\partial}{\partial a_{j-1}} + \sum_{k=0}^{p-1} (p-k) a_{k+1} \frac{\partial^2}{\partial a_j \partial a_k} \Big],$$

$$O\Omega = \sum_{k=0}^{p-1} (p-k) a_{k+1} \Big[(k+1) \frac{\partial}{\partial a_{k+1}} + \sum_{j=1}^{p} j a_{j-1} \frac{\partial^2}{\partial a_k \partial a_j} \Big].$$

$\Omega O - O\Omega$ enthält offenbar nur erste Ableitungen und heißt der Kommutator von Ω und O. In den ersten Gliedern von ΩO setze man $j = i+1$, in denen von $O\Omega$ hingegen $k = i-1$. Dann ist

$$\Omega O - O\Omega = \sum_{i=0}^{p-1} (i+1) a_i (p-i) \frac{\partial}{\partial a_i} - \sum_{i=1}^{p} (p-i+1) a_i \cdot i \cdot \frac{\partial}{\partial a_i}$$

$$= \sum_{i=0}^{p} (p-2i) a_i \frac{\partial}{\partial a_i}.$$

Wenn S eine homogene Funktion von $a_0, \ldots, a_p$ vom Grade d und daher eine Summe von Gliedern der Art

$$t \equiv c a_0^{e_0} a_1^{e_1}, \ldots, a_p^{e_p} \quad (e_0 + e_1 + \cdots + e_p = d)$$

ist, so bestätigen wir leicht den Eulerschen Satz (vgl. auch 5., Beisp. 3)

$$\sum_{i=0}^{p} a_i \frac{\partial S}{\partial a_i} \equiv dS.$$

Ist S außerdem noch isobar, so ist es eine Summe solcher Glieder t, für die $e_1 + 2e_2 + \cdots + pe_p = w$

konstant ist, und es ist dann

$$\sum_{i=0}^{p} i a_i \frac{\partial t}{\partial a_i} \equiv \sum_{i=0}^{p} i e_i t \equiv wt \quad \text{und daher auch} \quad \sum_{i=0}^{p} i a_i \frac{\partial S}{\partial a_i} \equiv wS.$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Durch Zusammenfassung erhält man

Satz 2: Wenn S in $a_0, \ldots, a_p$ homogen (vom Grade d) und isobar (vom Gewicht w) ist, so ist

$$(8) \qquad (\Omega O - O\Omega)S \equiv nS, \quad \text{wo} \quad n = pd - 2w,$$

$$(9) \qquad (\Omega O^r - O^r\Omega)S \equiv r(n - r + 1)O^{r-1}S.$$

Um letzteres für r induktiv zu beweisen, nehmen wir an, es gelte für $r = k$. Ersetzt man dann in (9) S durch OS, so muß n durch $n - 2$ ersetzt werden, da OS vom Grade d und vom Gewicht $w + 1$ ist. Dann folgt

$$\begin{aligned}(\Omega O^{k+1} - O^{k+1}\Omega)S &\equiv (\Omega O^k - O^k\Omega)OS + O^k(\Omega O - O\Omega)S \\ &\equiv k(n - 2 - k + 1)O^{k-1}OS + nO^kS \\ &\equiv (k + 1)(n - k)O^kS.\end{aligned}$$

Der Satz stimmt daher auch für $r = k + 1$ und ist damit bewiesen.

Ähnlich gilt, da ΩS vom Grade d und Gewicht $w - 1$ ist,

$$(10) \qquad (O\Omega^r - \Omega^r O)S \equiv r(-n - r + 1)\Omega^{r-1}S.$$

16. Existenzbeweis für eine Kovariante mit gegebenem seminvariantem Leitglied. In 12. bestätigten wir für die Fälle $p \leqq 4$, daß jede Seminvariante einer binären Form f $p$ter Ordnung das Leitglied einer Kovariante von f ist. Wir werden diesen Satz nunmehr für jedes p beweisen.

Hilfssatz: Wenn S eine nichtidentisch verschwindende Seminvariante einer binären p-ik vom Grade d und Gewicht w ist, so ist $pd - 2w \geqq 0$.

Angenommen, S sei eine Seminvariante mit negativem $n = pd - 2w$. Wegen $\Omega S \equiv 0$ folgt dann aus (9)

$$(11) \qquad \Omega O^r S = r(n - r + 1)O^{r-1}S \quad \text{für} \quad r = 1, 2, \ldots,$$

wo keiner der Koeffizienten rechts verschwindet. Erinnern wir uns jetzt daran, daß das Gewicht von OP um eins größer ist als das von P, so sehen wir, daß $O^{pd-w+1}S$, welches vom Grade d und Gewicht $pd + 1$ ist, identisch verschwindet, da das Maximalgewicht eines Polynoms in $a_0, \ldots, a_p$ vom Grade d gleich pd ist. Aus (11) folgt dann, daß auch $O^{pd-w}S \equiv 0$[1]), und durch wiederholte Anwendung von (11) erhält man schließlich $OS \equiv 0$, d. h. $S \equiv 0$ gegen die Voraussetzung. —

1) Da $pd - w = 0$ der Voraussetzung $S \neq 0$ widerspricht, so muß $pd - w > 0$ sein.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Nach 12. hat jede Kovariante

$$K = Sx^n + S_1 x^{n-1} y + S_2 x^{n-2} y^2 + \cdots + S_n y^n$$

mit dem Leitgliede S die Ordnung $n = pd - 2w$. Wendet man den Operator (7) auf K an, so erhält man den Ausdruck

$$(OS - S_1) x^n + (OS_1 - 2S_2) x^{n-1} y + \cdots + (OS_{n-1} - nS_n) x y^{n-1} + OS_n y^n,$$

welcher dann und nur dann identisch in x und y verschwindet, wenn

$$(12) \quad K = Sx^n + OSx^{n-1} + \frac{1}{2} O^2 S x^{n-2} y^2 + \cdots + \frac{1}{n!} O^n S y^n$$

und $O^{n+1} S \equiv 0$. Um zu zeigen, daß letztere Bedingung erfüllt ist, wenn S eine Seminvariante und $n = pd - 2w$ ist, beachte man, daß (11) für $r = n + 1$ die Identität $\Omega O^{n+1} S \equiv 0$ ergibt. Da $O^{n+1} S$ vom Grade d und Gewicht $W = w + n + 1 = pd - w + 1$ ist und durch Anwendung von Ω verschwindet, ist es nach 14., Folgerung 2 eine Seminvariante und daher nach obigem Hilfssatz identisch Null, da $pd - 2W = -(pd - 2w) - 2 < 0$. Also wird (12) durch den Operator (7) annihiliert.

Das Gleiche gilt für den Operator (6), denn wendet man ihn auf (12) an, so ist der Koeffizient von $x^{n-r} y^r$ gleich

$$\frac{1}{r!} \Omega O^r S - \frac{1}{(r-1)!} (n - r + 1) O^{r-1} S$$

und daher nach (11) identisch Null. Satz 1 zeigt dann, daß (12) eine Kovariante ist.

Satz 3: Es gibt immer eine, aber auch nur eine Kovariante einer binären p-ik, deren Leitglied eine gegebene Seminvariante der p-ik ist.

17. Der Hilbertsche Satz: Jedes System S endlich oder unendlich vieler Formen in $x_1, \ldots, x_n$ enthält eine endliche Zahl von Formen $F_1, \ldots, F_k$, so daß sich jede Form F des Systems darstellen läßt als lineare Kombination von $F_1, \ldots, F_k$ mit Koeffizienten, welche wieder Formen in $x_1, \ldots, x_n$ sind, aber nicht notwendig zu S gehören:

$$F \equiv A_1 F_1 + \cdots + A_k F_k.$$

$F_1, \ldots, F_k$ heißt eine Basis des Systems.[1])

1) Hilbert, Mathem. Annalen 36 (1890), p. 473.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Für $n = 1$ besteht S aus gewissen Formen $c_1 x^{e_1}, c_2 x^{e_2}, \ldots$ Ist e_m der niedrigste vorkommende Exponent und $F_1 = c_m x^{e_m}$, so ist jede Form aus S das Produkt von F_1 und einem Ausdruck wie $k x^e$, wo $e \geqq 0$. Daher gilt der Satz für $n = 1$.

Um ihn allgemein zu beweisen, nehmen wir ihn für jedes System in $n - 1$ Variabeln als richtig an. Ferner dürfen wir voraussetzen, daß in S eine Form F_0 von der Ordnung r vorkommt, in welcher der Koeffizient von x_n^r von Null verschieden ist. Denn wenn $f(x_1, \ldots, x_n)$ eine Form aus S ist, welche x_n enthält, so wird, wenn $c_1, \ldots, c_n (c_n \neq 0)$ Zahlen sind, für die

$$c = f(c_1, \ldots, c_n) \neq 0$$

ist, f durch die Transformation

$$T: x_i = y_i + c_i y_n \ (i = 1, \ldots, n-1), \qquad x_n = c_n y_n$$

mit der Determinante $c_n \neq 0$ in die Form $F_0(y_1, \ldots, y_n)$ übergeführt, in welcher der Koeffizient von y_n^r offenbar c, also $\neq 0$ ist. Transformiere ich also alle Formen von S mit T, so bekomme ich ein System S', für welches die obige Voraussetzung gilt. Hat aber S' eine Basis, so daß also $F' \equiv A_1' F_1' + \cdots + A_k' F_k'$, so bekomme ich durch Ausführung der umgekehrten Transformation T^{-1} aus jedem F' wieder F und weiter $F \equiv A_1 F_1 + \cdots + A_k F_k$, so daß auch S eine Basis besitzt.

Dividiert man jetzt irgend ein F aus S durch F_0, so sei $F \equiv F_0 P + R$, wo der Rest R eine Form ist, deren Ordnung in x_n kleiner als r ist. In R fassen wir die Glieder, welche x_n genau im Grade $r - 1$ enthalten, zusammen und bekommen

$$F \equiv F_0 P + M x_n^{r-1} + N,$$

wo M eine Form in $x_1, \ldots, x_{n-1}$ ist, während N eine Form in $x_1, \ldots, x_n$ vom Grade $\leqq r - 2$ in x_n ist. Jede Form F bestimmt eindeutig ein M.

Da der Satz (nach Voraussetzung) für das System M gültig ist, so besitzt M eine Basis $M_1, \ldots, M_l$, welche gewissen Formen $F_1, \ldots, F_l$ von S entsprechen, so daß also für jedes M

$$M \equiv f_1 M_1 + \cdots + f_l M_l,$$

wo die f_i natürlich Formen in $x_1, \ldots, x_{n-1}$ sind.

Dann ist $$F \equiv F_0 P + N + x_n^{r-1} \sum_{i=1}^{l} f_i M_i.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Greift man diejenigen F_i heraus, aus denen sich die M_i ergeben haben, so gilt auch für sie

$$F_i \equiv F_0 P_i + M_i x_n^{r-1} + N_i \qquad (i = 1, \ldots, l).$$

Eliminiert man nun hiermit aus der obigen Identität die M_i, so erhält man

$$F \equiv F_0 P' + \sum f_i F_i + R',$$

wo

$$P' = P - \sum f_i P_i, \quad R' = N - \sum f_i N_i$$

ist. Jeder Exponent von x_n in R' ist $\leqq r-2$; wir greifen die Glieder, in denen dieser Exponent genau $r-2$ ist, heraus und bekommen

$$F = F_0 P' + \sum_{i=1}^{l} f_i F_i + M' x_n^{r-2} + N',$$

wo M' eine Form in $x_1, \ldots, x_{n-1}$ und N' eine solche in $x_1, \ldots, x_n$ ist, deren Ordnung in x_n höchstens $r-3$ ist.

Da der Satz für das System M' gilt, so ist jedes M' eine lineare Kombination von $M_1', \ldots, M_m'$, welche gewissen Formen $F_{l+1}, \ldots, F_{l+m}$ von S entsprechen. Wie oben unterscheidet sich F von einer linearen Kombination der $F_0, \ldots, F_{l+m}$ durch $M'' x_n^{r-3} + N''$, wo M'' eine Form in $x_1, \ldots, x_{n-1}$ und N'' eine Form ist, deren Grad in x_n höchstens $r-4$ beträgt. Durch Fortsetzung dieses Verfahrens sehen wir, daß sich F von einer linearen Kombination gewisser Formen $F_0, \ldots, F_t$ von S nur durch eine von x_n freie Form unterscheidet. — Ein weiterer Schritt führt dann zum Ziel.

18. Die Endlichkeit des Formensystems. Der Einfachheit halber betrachten wir zunächst nur Invarianten einer einzelnen binären Form f mit den Koeffizienten $a_0, \ldots, a_p$. Nach Satz 8 in 8. ist jede Invariante I von f homogen in den a. Nach obigem Satz hat das System der Invarianten I eine Basis $I_1, \ldots, I_m$, so daß also

$$I \equiv E_1 I_1 + \cdots + E_m I_m. \tag{13}$$

I und I_k seien vom Grade d bzw. d_k. Nach 10. sind ihre Gewichte $\frac{1}{2}pd$ bzw. $\frac{1}{2}pd_k$, so daß E_k den Grad $D_k = d - d_k$ und das Gewicht $\frac{1}{2}pD_k$ besitzt.

Wir werden nun zunächst einen Differentialoperator D bilden, der E_k zu einer Invarianten macht. Wendet man auf (10) den Operator O^{r-2} an, so erhält man

$$O^{r-1}\Omega^r S - O^{r-2}\Omega^r O S \equiv r(-n-r+1) O^{r-2}\Omega^{r-1} S.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ersetzt man im zweiten Gliede $\Omega O S$ durch seinen aus (8) folgenden Wert $O\Omega S + nS$, so ist

$$O^{r-1}\Omega^r S \equiv O^{r-2}\Omega^{r-1}[O\Omega - (r-1)(n+r)]S.$$

Da $O\Omega S$ von gleichem Grad und Gewicht wie S ist, so können wir die Formel, die wir aus der obigen durch Ersetzen von r durch $r-1$ erhalten, anwenden, um $O^{r-2}\Omega^{r-1}$ zu eliminieren. Durch Wiederholung dieses Prozesses bekommen wir

$$O^{r-1}\Omega^r S \equiv \Omega[O\Omega - (n+2)][O\Omega - 2(n+3)]\cdots [O\Omega - (r-1)(n+r)]S,$$

eine Formel, die wir auch durch Induktion bestätigen können. Wenn nun S vom Gewichte $w = \frac{1}{2}p\delta$ und vom Grade δ ist, so ist in (8) $n = 0$. Setzt man jetzt $r = w+1$, dividiert durch $(-2)\cdot(-2\cdot 3)\cdots$, so bekommt man wegen $\Omega^{w+1}S \equiv 0$ auch $\Omega D S \equiv 0$, wo

$$D = \left[1 - \frac{O\Omega}{1\cdot 2}\right]\left[1 - \frac{O\Omega}{2\cdot 3}\right]\cdots\left[1 - \frac{O\Omega}{w(w+1)}\right]. \tag{14}$$

Da nun DS durch Anwendung von Ω verschwindet und von konstantem Grade δ und konstantem Gewicht $w = \frac{1}{2}p\delta$ ist, so ist es nach 14., Folgerung 2 eine Seminvariante, und, da es das Leitglied einer Kovariante von der Ordnung $n = 0$ ist, sogar eine Invariante. Damit haben wir in D den gesuchten Operator, der aus S eine Invariante hervorgehen läßt. — Da ferner die Invarianten I und I_k durch Ω und O annihiliert werden, so ist $D(EI) = I\cdot(DE) + E\cdot(DI) = I\cdot(DE)$. Diese Resultate gelten auch, wenn wir auf der rechten Seite von (14) Faktoren wie $g = 1 - cO\Omega$ hinzufügen, da gS von gleichem Grad und Gewicht wie S ist. Nehmen wir daher an, das größte Gewicht aller E_k sei w, und operieren mit dem entsprechenden D an (13), so erhalten wir jetzt

$$I \equiv J_1 I_1 + \cdots + J_m I_m,$$

wo $J_k = DE_k$ eine Invariante ist. — Da jedes J_k wieder von der Form (13) ist, d. h.

$$J_k = \sum_{i=1}^{m} e_{ik} I_i,$$

so ist

$$I \equiv \sum e_{ik} I_i I_k.$$

Wenden wir hierauf noch einmal einen Operator D mit hinreichend großem w an, so bekommen wir

$$I \equiv \sum L_{jk} I_j I_k,$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

wo die L_{jk} Invarianten von f sind. Da bei diesem Prozeß mit jedem Schritt eine Erniedrigung des Grades eintritt, so bekommen wir schließlich für I ein Polynom in $I_1, \ldots, I_m$ mit Zahlenkoeffizienten. Daher bilden $I_1, \ldots, I_m$ ein vollständiges System von Invarianten von f.

Übung: Man dehne den Endlichkeitsbeweis auf Invarianten eines Systems binärer Formen $a_0 x^{p_1} + \cdots$, $b_0 x^{p_2} + \cdots$, $c_0 x^{p_3} + \cdots$, aus. Zuerst beweise man, wie in 14, daß eine Invariante durch Anwendung von

$$\Sigma\Omega = a_0 \frac{\partial}{\partial a_1} + \cdots + b_0 \frac{\partial}{\partial b_1} + \cdots + p_2 b_{p_2-1} \frac{\partial}{\partial b_{p_2}} + c_0 \frac{\partial}{\partial c_1} + \cdots$$

und von ΣO verschwindet. Wenn dann S ein Polynom in den $a_i, b_i, \ldots$ von konstantem Grade d_1 in den a, von konstantem Grade d_2 in den $b, \ldots$ und von konstantem Gesamtgewicht w in den $a, b, \ldots$ ist, so zeige man, daß (8) und (10) bestehen bleiben, wenn wir O durch ΣO, Ω^r durch $(\Sigma\Omega)^r$ und n durch $\Sigma p_i d_i - 2w$ ersetzen. — Den Operator (14) verallgemeinere man auf die gleiche Weise.

Der Endlichkeitsbeweis läßt sich durch folgenden Hilfssatz auf Kovarianten ausdehnen:

Hilfssatz: Das System aller homogenen Kovarianten der binären Formen $f_1, \ldots, f_k$ ist identisch mit dem Formensystem, das man aus den (in X, Y homogenen) Invarianten I von $f_1, \ldots, f_k$ und $L \equiv Yx - Xy$ bekommt, wenn man in jedem I X durch x und Y durch y ersetzt.

Der Einfachheit halber bezeichne man die Koefizienten von $f_1, \ldots, f_k$ in irgendeiner Ordnung mit $a, b, \ldots A, B, \ldots$. seien die Koeffizienten der durch die Transformation

$$x = pu + qv, \quad y = ru + sv, \quad D = ps - qr \neq 0$$

erhaltenen Formen. Sie ersetzt L durch $Vu - Uv$, wo

$$U = sX - qY, \quad V = -rX + pY$$

oder umgekehrt

$$DX = pU + qV, \quad DY = rU + sV.$$

Wenn nun $I = I(a, b, \ldots; X, Y)$ das Gewicht l hat, so ist

$$I(A, B, \ldots; U, V) = D^l I = D^{l-n} I(a, b, \ldots; DX, DY),$$

da I von konstanter Ordnung n in X, Y ist. Daher ist identisch in U, V

$$I(A, B, \ldots; U, V) \equiv D^{l-n} I(a, b, \ldots; pU + gV, rU + sV)$$

oder, wenn wir U, V durch u, v ersetzen

$$I(A, B, \ldots; u, v) \equiv D^{l-n} I(a, b, \ldots; x, y),$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

so daß also $I(a, b, \ldots; x, y)$ eine Kovariante von $f_1, \ldots, f_k$ von der Ordnung n und dem Gewicht $i - n$ ist. — Da der Beweis sich auch umkehren läßt und da jede Kovariante eine Summe von lauter in den Variabeln homogenen Kovarianten ist (8.), so haben wir vollständig den

Satz 5: Jedes System binärer Formen besitzt ein vollständiges System von Kovarianten.

Der erste Beweis dieses klassischen Satzes wurde von Gordan mit Hilfe der Symbolik gefunden. Infolge eines Fehlers, der sich auf die Unabhängigkeit der Syzygien zwischen den Kovarianten bezog, war Cayley vorher zu dem entgegengesetzten Ergebnis gekommen, daß nämlich das Fundamentalsystem einer binären Form fünfter Ordnung unbegrenzt sei. — Für binäre Formen bis zur vierten Ordnung haben wir in 12. ein vollständiges System von Kovarianten aufgestellt.

19. Endlichkeit der Syzygien. $I_1, \ldots, I_m$ sei ein vollständiges System von Invarianten der binären Formen $f_1, \ldots, f_r$. $S(z_1, \ldots, z_m)$ sei ein Polynom mit numerischen Koeffizienten von der Art, daß $S(I_1, \ldots, I_m)$ in den Koeffizienten der f identisch verschwindet. Dann heißt $S(I_1, \ldots, I_m) = 0$ eine Syzygie zwischen den Invarianten (vgl. die Beispiele in 12.).

Durch Einführung einer neuen Variabeln z_{m+1} können wir $S(z_1, \ldots, z_m)$ in eine homogene Form H verwandeln, indem wir alle Glieder von nichtmaximalem Grade mit einer passenden Potenz von z_{m+1} multiplizieren. Nach dem Hilbertschen Satz sind alle Formen H durch eine endliche Zahl $H_1, \ldots, H_k$ von ihnen linear darstellbar. Setzt man hinterher dann $z_{m+1} = 1$, so wird

$$S \equiv P_1 S_1 + \cdots + P_k S_k, \tag{15}$$

wo die P Polynome in den z sind. In dieser Identität in $z_1, \ldots, z_{m+1}$ können wir schließlich $z_1 = I_1, \ldots, z_m = I_m$ setzen und erhalten so

Satz 6: Es existiert eine endliche Zahl von Syzygien

$$S_1 = 0, \ldots, S_k = 0,$$

aus denen sich jede andere Syzygie als lineare Kombination ergibt, in der die Koeffizienten Invarianten sind.

Jede Syzygie ist also eine Folge von $S_1 = 0, \ldots, S_k = 0$. — Wegen des Hilfssatzes in 18. gilt der Beweis auch für Syzygien zwischen Kovarianten.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

20. Kanonische Form einer binären Form ungrader Ordnung. In 7. sahen wir, daß jede binäre kubische Form mit nichtverschwindender Diskriminante die Summe der Kuben zweier Linearformen ist, welche die Faktoren der Hesseschen Form sind. Wir werden jetzt einen entsprechenden Satz für Formen von irgendeiner ungraden Ordnung beweisen. — In (1) sei also $p = 2n - 1$. Wir suchen solche Konstanten p_i, r_i, daß

$$(16) \qquad f \equiv p_1(x + r_1 y)^{2n-1} + \cdots + p_n(x + r_n y)^{2n-1}.$$

Die Bedingungen für die p und r sind offenbar

$$(17) \qquad a_i = p_1 r_1^i + \cdots + p_n r_n^i \qquad (i = 0, 1, \ldots, 2n-1).$$

Die n linearen Gleichungen

$$(18) \qquad a_s q_n + a_{s+1} q_{n-1} + \cdots + a_{s+n-1} q_1 + a_{s+n} = 0 \qquad (s = 0, 1, \ldots, n-1)$$

lassen sich, wenn die Determinante ihrer Koeffizienten nicht verschwindet, nach $q_n, \ldots, q_1$ auflösen. Ferner seien $r_1, \ldots, r_n$ die Wurzeln von

$$(19) \qquad \varphi(z) = z^n + q_1 z^{n-1} + \cdots + q_{n-1} z + q_n = 0.$$

Wenn die $r_1, \ldots, r_n$ voneinander verschieden sind[1]), so sind die $p_1, \ldots, p_n$ durch die Bedingungen (17) für $i = 0, 1, \ldots, n-1$ eindeutig bestimmt. Um zu beweisen, daß dann auch die übrigen Bedingungen erfüllt sind, nehmen wir die Bedingungen (17) für $i < s + n$ als bewiesen an und zeigen, daß dann auch die Bedingung für $i = s + n$ erfüllt ist. Dazu multipliziere man die Bedingungsgleichungen für $i = s, s + 1, \ldots, s + n - 1, s + n$ nach einander mit $q_n, q_{n-1}, \ldots, q_1, 1$ und addiere. Auf der linken Seite ist dann der Koeffizient von p_k gleich

$$r_k^s q_n + r_k^{s+1} q_{n-1} + \cdots + r_k^{s+n-1} q_1 + r_k^{s+n} = r_k^s \cdot \varphi(r_k) = 0$$

und, da auch die linke Seite wegen (18) verschwindet, so war auch die Bedingung für $i = s + n$ erfüllt.

Die Gleichung mit den Wurzeln $r_1, \ldots, r_n$ erhält man offenbar durch Elimination der q aus (18) und (19). Wir ziehen die in x und y homogene Gleichung, deren Linearfaktoren $x + r_i y$ sind, vor. Man findet sie als Determinante der Koeffizienten von $q_n, \ldots, q_1, 1$ in den Gleichungen (18) und

$$(19') \qquad y^n q_n - x y^{n-1} q_{n-1} + x^2 y^{n-2} q_{n-2} - \cdots + (-x)^{n-1} y q_1 + (-x)^n = 0$$

1) Sind sie es nicht oder verschwindet die Determinante, so ist die Form f nicht allgemein und soll daher von der Behandlung ausgeschlossen werden.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Sie ist also gleich

$$\begin{vmatrix} y^n & -xy^{n-1} & x^2y^{n-2} & \dots & (-x)^{n-1}y & (-x)^n \\ a_0 & a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_1 & a_2 & a_3 & \dots & a_n & a_{n+1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n-1} & a_n & a_{n+1} & \dots & a_{2n-2} & a_{2n-1} \end{vmatrix} = 0$$

und heißt die Kanonizante C von f.

Satz 7: Jede hinreichend allgemeine binäre Form von der ungraden Ordnung $2n - 1$ läßt sich als Potenzsumme von n Linearfaktoren darstellen.

Übungen: 1. Für $n = 3$ ist der Koeffizient von x^3 in der Kanonizante C der Form f fünfter Ordnung die Invariante J der biquadratischen Form $q = a_0x^4 + 4a_1x^3y + \cdots$, also erst recht eine Seminvariante von q und wird daher durch den Operator Ω in (6), in dem $p = 4$ gesetzt wird, zum Verschwinden gebracht. Da aber a_5 in J überhaupt nicht vorkommt, so verschwindet J auch durch Ω für $p = 5$ und ist daher eine Seminvariante von f.

2. Man zeige, daß J, da es eine rationale Funktion der Seminvarianten a_0, S_2, S_3, S_4 ist, eine Seminvariante jeder Form von mindestens vierter Ordnung ist. (Vgl. 12., (21) und 10.).

3. Es gibt eine Kovariante dritter Ordnung der Form f fünfter Ordnung mit dem Leitgliede J. Sie fällt mit C zusammen, da die Kanonizante der aus f durch irgendeine lineare Transformation T abgeleiteten Form als Faktoren die durch T transformierten Linearfaktoren von C besitzt.

4. Für $n = 3$ ist die Kanonizante C von f der Minor von y^3 in Δ, wo

$$\Delta = \begin{vmatrix} y^3 & 0 & 0 & 0 \\ a_0 & a_0x + a_1y & a_1x + a_2y & a_2x + a_3y \\ a_1 & a_1x + a_2y & a_2x + a_3y & a_3x + a_4y \\ a_2 & a_2x + a_3y & a_3x + a_4y & a_4x + a_5y \end{vmatrix}.$$

Denn das Produkt von C und $D = \begin{vmatrix} 1 & x & 0 & 0 \\ 0 & y & x & 0 \\ 0 & 0 & y & x \\ 0 & 0 & 0 & y \end{vmatrix} = y^3$, Zeilen mit Spalten multipliziert, ergibt Δ.

Ein ähnliches Resultat gilt auch im allgemeinen Fall.

5. Wenn eine Seminvariante einer Form fünfter Ordnung a_5 nicht enthält, so ist sie eine Seminvariante der Form q von der Ordnung 4. — Ist das Gewicht doppelt so groß wie sein Grad, so ist S eine Invariante von q. (Vgl. Satz 12 in Kap. 1.)

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

6. Man finde die Determinante, deren Verschwinden notwendig und hinreichend dafür ist, daß eine binäre Form von der Ordnung $2n$ eine Summe der $2n$ten Potenzen von n Linearformen sind.

Anleitung: Man wende (18) auch für $s = n$ an.

21. Weitere Probleme. Zum Schluß verweisen wir noch auf folgende Probleme:

Außer der von uns angewandten Methode zur Behandlung der Invariantentheorie, die im Wesentlichen eine Methode mittels Differentialoperatoren ist, gibt es noch eine andere, die lange Zeit, besonders in Deutschland, die herrschende war: die symbolische Methode. Sie wurde (von Cayley und in brauchbarerer Gestalt) von Aronhold begonnen und von Clebsch und anderen zu einem hohen Vollkommenheitsgrad ausgebildet. Sie war lange Zeit das algebraische Hilfsmittel der Geometrie.[1])

Darstellung von Formen durch eine Summe von Potenzen linearer Formen.[2])

Seminvarianten und Kovarianten als Funktionen der Wurzeldifferenzen.[3])

Interessante Anwendungen der Invarianten einer Form fünfter Ordnung finden sich in den elementaren Abhandlungen, die in 112. zitiert sind.

---

1) Außer den am Ende des ersten Kapitels genannten Originalarbeiten und Lehrbüchern vergleiche man das inhaltsreiche Buch von R. Weitzenböck: Invariantentheorie, Groningen 1923. (Deutsch.)

2) Vgl. die Arbeiten von Rosanes, Crelles Journal (76) und bes. von Reye, (Crelles Journal (78). Unter den neueren Arbeiten die der Italiener, bes. die von Palatini, Atti della R. Acc. di Torino (38), 1902 und Rendic. Acc. Lincei, ser. 5a (12), 1903 und von Terracini, Annali matem. (24), 1915 und Atti Acc. Torino (51), 1915.

3) Dickson, Algebraic Invariants, Wiley Sons, 1914, pp. 53—58.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

DRITTES KAPITEL

MATRIZEN, BILINEARE FORMEN, LINEARE GLEICHUNGEN

In den folgenden Kapiteln III—VII, die unabhängig von den beiden ersten sind, geben wir eine neue Darstellung der Gegenstände, die man gewöhnlich „Höhere Algebra" nennt. Zuerst entwickeln wir den Cayleyschen Matrizenkalkul und die damit im wesentlichen äquivalente Theorie der bilinearen Formen. Wir werden dabei die Hauptsätze über die Lösung von Systemen linearer Gleichungen nicht voraussetzen, sondern sie bei unserer Darstellung als Folgerungen bekommen.

22. Lineare Formen, Matrizen, lineare Transformationen. Jede homogene lineare Funktion, wie $7x - 3y$, heißt eine lineare Form. Wir gehen von m solchen linearen Formen

$$(1) \qquad \begin{cases} l_1 = a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n, \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ l_m = a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{mn}y_n \end{cases}$$

in den n Variabeln $y_1, \ldots, y_n$ aus und schreiben die Koeffizienten der aufeinanderfolgenden linearen Formen in die aufeinanderfolgenden Reihen der Tafel:

$$(2) \qquad A = \begin{pmatrix} a_{11}, & a_{12} \ldots a_{1n} \\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ a_{m1}, & a_{m2} \ldots a_{mn} \end{pmatrix}.$$

Eine solche rechteckige Tafel mit mn Gliedern heißt eine Matrix von m Zeilen und n Spalten oder kurz eine mn-Matrix. Die a_{ij} heißen die Elemente der Matrix. Wir werden A die Matrix der (Koeffizienten der) linearen Formen (1) nennen.

Beispiele für einreihige Matrizen sind die Bezeichnungen (x, y) und (x, y, z) für Punkte der Ebene oder des Raumes, so daß also die Elemente dieser Matrizen die Koordinaten der Punkte sind.

Die Matrix (2) heißt der mn-Matrix

$$\begin{pmatrix} d_{11}, & d_{12} \ldots d_{1n} \\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot \\ d_{m1}, & d_{m2} \ldots d_{mn} \end{pmatrix}$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

dann und nur dann gleich, wenn entsprechende Elemente gleich sind, also wenn

$$a_{11} = d_{11}, \quad a_{12} = d_{12}, \quad \ldots \quad a_{mn} = d_{mn}.$$

Wir werden für (1) und (2) auch kurz schreiben

$$(1') \qquad l_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, m),$$

$$(2') \qquad A = (a_{ij}) \qquad (i = 1, \ldots, m;\ j = 1, \ldots, n),$$

wo wir also das Element a_{ij} der $i$ten Zeile und $j$ten Spalte der Matrix (2) herausheben.

Nehmen wir nun an, die n Variabeln y_j seien linear in den s neuen Variabeln $z_1, \ldots, z_s$ ausdrückbar:

$$(3) \qquad y_j = \sum_{k=1}^{s} b_{jk} z_k \qquad (j = 1, \ldots, n),$$

und setzen diese Werte in (1') ein, so erhalten wir

$$(4) \qquad l_i = \sum_{j=1}^{n} \sum_{k=1}^{s} a_{ij} b_{jk} z_k = \sum_{k=1}^{s} p_{ik} z_k \qquad (i = 1, \ldots, m),$$

wo

$$(5) \qquad p_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} \qquad (i = 1, \ldots, m;\ k = 1, \ldots, s).$$

(Das Bildungsgesetz der rechten Seite ist, wie man sieht, ganz einfach: Der Summationsbuchstabe kommt in die Mitte, die Indizes i und k von p_{ik} an die Außenseiten.) Die Matrizen der linearen Formen (3) und (4), d. h.

$$(6) \qquad B = \begin{pmatrix} b_{11} \ldots b_{1s} \\ \ldots \\ b_{n1} \ldots b_{ns} \end{pmatrix}, \quad P = \begin{pmatrix} p_{11} \ldots p_{1s} \\ \ldots \\ p_{m1} \ldots p_{ms} \end{pmatrix}$$

seien wieder kurz mit $B = (b_{ik})$ und $P = (p_{ik})$ bezeichnet.

P heißt das **Produkt** von A und B (in dieser Ordnung genommen) und wird mit $P = AB$ bezeichnet.

Mit Rücksicht auf (5) haben wir daher die folgende

Multiplikationsregel für Matrizen. Das Element in der $i$ten Zeile und $k$ten Spalte des Produkts einer Matrize A mit n Spalten und einer Matrix B mit n Zeilen ist die Summe der Produkte der sukzessiven Elemente der $i$ten Zeile von A und der entsprechenden Elemente der $k$ten Spalte von B.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Z. B. $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma, & a\beta + b\delta \\ c\alpha + d\gamma, & c\beta + d\delta \end{pmatrix}. \quad -$$

Unter einer linearen Transformation verstehen wir ein System von n linearen homogenen Gleichungen

$$y_j = \sum_{k=1}^{n} b_{jk} z_k \qquad (j = 1, \ldots, n), \tag{7}$$

welches die Variabeln $y_1, \ldots, y_n$ linear durch dieselbe Zahl von Variabeln $z_1, \ldots, z_n$ ausdrückt. Die Transformation hat die Matrix (b_{ik}). Setzt man in (3) bis (6) $s = n$, so sagen wir, daß die Transformation (7) das System linearer Formen (1) durch das System linearer Formen (4) ersetzt. Damit haben wir

Satz 1: Eine lineare Transformation mit der Matrix B ersetzt ein System linearer Formen mit der Matrix A durch ein System linearer Formen mit der Matrix AB.

Für $m = n$ definieren die Gleichungen (1′) eine lineare Transformation

$$l_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, n). \tag{8}$$

Die zugehörige Transformation (4) mit der Matrix AB drückt dann $l_1, \ldots, l_n$ linear durch $z_1, \ldots, z_n$ aus und heißt das Produkt der beiden Transformationen (A) und (B).

Die ein-eindeutige Beziehung zwischen linearen Transformationen und quadratischen Matrizen wird daher durch die Multiplikation nicht zerstört. Aus diesem Grunde wird eine lineare Transformation dann, wenn die spezielle Bezeichnung der Variabeln unwesentlich ist, einfach durch ihre Matrix bezeichnet.

Die Determinante $|a_{ij}|$ heißt die Determinante der Transformation. Da obige Regel für die Multiplikation quadratischer Matrizen eine der Multiplikationsregeln für die Determinanten ist, so schließen wir daraus, daß die Determinante des Produkts zweier linearer Transformationen gleich dem Produkt ihrer Determinanten ist.

Eine lineare Transformation heißt nichtsingulär, wenn ihre Determinante von Null verschieden ist, im anderen Falle singulär.

23. Inverse, skalare, adjungierte Matrix; Einheitsmatrix. Die Determinante der Transformation (8) bezeichne man mit a. Für $a \neq 0$ besitzen die Gleichungen (8) die einzige Lösung

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$$(9) \qquad y_j = \sum_{k=1}^{n} \frac{A_{kj}}{a} l_k \qquad (j = 1, \ldots, n),$$

wo A_{kj} die Unterdeterminante zu a_{kj} in a bezeichnet. Die Gleichungen (9) definieren eine lineare Transformation, welche die y durch die l ausdrückt. Sie heißt die zu (8) inverse Transformation. Da die Bezeichnung der Buchstaben unwesentlich ist, ersetzen wir l_k durch z_k. Dann definiert offenbar des Produkt von (8) und ihrer inversen Transformation

$$(9') \qquad y_j = \sum_{k=1}^{n} \frac{A_{kj}}{a} z_k \qquad (j = 1, \ldots, n)$$

die identische Transformation E:

$$(10) \qquad l_1 = z_1, \ldots, l_n = z_n.$$

Die inverse zu (9) ist offenbar wieder die Ausgangstransformation (8). — Führt man für

$$(11) \qquad u_1 = tv_1, \ldots, u_n = tv_n$$

die Bezeichnung S_t ein und multipliziert (8) in irgendeiner Reihenfolge mit S_t, so erhält man das Produkt

$$l_i = \sum_{j=1}^{n} t a_{ij} y_j \qquad (i = 1, \ldots, n),$$

dessen Matrix entweder mit tA oder At bezeichnet werden kann und das aus A hervorgeht, indem jedes Element mit t multipliziert wird. Die Matrix von (11) wird mit S_t bezeichnet und heißt eine skalare Matrix; ihre Diagonalelemente sind alle gleich t, die anderen Elemente gleich Null. Ein besonderer Fall ist die oben in (10) mit E bezeichnete Einheitsmatrix. Zusammengefaßt haben wir

$$(12) \qquad S_t A = A S_t = tA, \quad EA = AE = A.$$

Daher können wir in Produkten einen skalaren Matrizenfaktor S_t durch die Zahl t ersetzen und den Faktor E ganz weglassen.

Eine Matrix, deren Elemente alle gleich Null sind, heißt eine Nullmatrix und wird mit o bezeichnet. Nach (12) haben wir für $t = 0$ $oA = Ao = o$ für jede Matrix A.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Matrix in (9′) wird mit

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{a} & \cdots & \frac{A_{n1}}{a} \\ \cdot & \cdot & \cdot \\ \frac{A_{1n}}{a} & \cdots & \frac{A_{nn}}{a} \end{pmatrix} \tag{13}$$

bezeichnet und heißt zu A invers. Nach Obigem ist

$$A A^{-1} = A^{-1} A = E. \tag{14}$$

Unterdrücken wir in (13) die Nenner, so erhalten wir die sog. Adjungierte der Matrix A:

$$\text{Adj.}\, A = \begin{pmatrix} A_{11} & \cdots & A_{n1} \\ \cdot & \cdot & \cdot \\ A_{1n} & \cdots & A_{nn} \end{pmatrix}. \tag{15}$$

Das Element A_{ji} in der $i$ten Zeile und $j$ten Spalte der Adjungierten von A ist die Adjungierte von a_{ji} in A.

Falls $a = |a_{ij}| \neq 0$, haben wir nach Definition Adj. $A = a \cdot A^{-1}$; dann folgt sofort aus (14)

$$A \cdot (\text{Adj.}\, A) = (\text{Adj.}\, A) \cdot A = aE. \tag{16}$$

Dieses Resultat (16) besteht auch für $a = 0$, wie sich aus Stetigkeitseigenschaften ergibt oder sich durch direkte Multiplikation zeigen läßt.

24. Assoziatives und distributives Gesetz. Es seien $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ irgendwelche mn-, ns-, st-Matrizen. Nach (5) ist jedes Element $[ik]$ (der $i$ten Zeile und $k$ten Spalte) des Produktes AB von der Form $\Sigma a_{ij} b_{jk}$. Nach derselben Regel ist das Element $[il]$ von $(AB) \cdot C$ gleich

$$\sum_{k=1}^{s} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) c_{kl}. \tag{17}$$

Das Element $[jl]$ von BC ist $\Sigma b_{jk} c_{kl}$ und daher das Element $[il]$ von $A \cdot (BC)$ gleich

$$\sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{s} b_{jk} c_{kl} \right),$$

also gleich der Summe (17). So gilt

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 2: Die Multiplikation der Matrizen ist assoziativ[1]*), d. h. es ist*

$$(AB)\cdot C = A\cdot(BC). \tag{18}$$

Jedes dieser Produkte kann daher, ohne zu Irrtümern Veranlassung zu geben, mit ABC, ebenso $ABC\cdot D, AB\cdot CD, A\cdot BCD$ einfach mit $ABCD$ bezeichnet werden usw. Der Fall gleicher Faktoren zeigt, daß A^e bei positivem ganzen e eindeutig bestimmt ist. —

Als **Summe** (oder **Differenz**) **zweier mn-Matrizen** bezeichnet man die mn-Matrix, in der jedes Element die Summe (oder Differenz) der entsprechenden Elemente der gegebenen Matrizen ist. Z. B.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \pm \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a \pm \alpha, & b \pm \beta \\ c \pm \gamma, & d \pm \delta \end{pmatrix}.$$

Es ergibt sich sofort, daß

$$\begin{aligned} A + B &= B + A, \quad (A + B) + C = A + (B + C), \\ tA + tB &= t(A + B), \quad tA + uA = (t + u)A. \end{aligned} \tag{19}$$

Das Element $[ik]$ von $A(B + C)$ ist $\Sigma a_{ij}(b_{jk} + c_{jk})$, also die Summe der Elemente $[ik]$ von AB und AC. So haben wir

Satz 3: Die Multiplikation der Matrizen ist distributiv, d. h. es ist

$$A(B \pm C) = AB \pm AC, \quad (B \pm C)A = BA \pm CA. \tag{20}$$

Wegen des assoziativen Gesetzes ist die Inverse eines Produkts gleich dem Produkt der in umgekehrter Reihenfolge multiplizierten Inversen der Faktoren. Denn es ist z. B. $ABC\cdot C^{-1}B^{-1}A^{-1} = A\cdot BB^{-1}\cdot A^{-1} = E$.

Wenn A nicht-singulär ist, so hat die Gleichung $AX = B$ die einzige Lösung $X = A^{-1}B$, während $YA = B$ die Lösung $Y = BA^{-1}$ hat. Da die Multiplikation der Matrizen nicht kommutativ ist (im allgemeinen), so ist $X \neq Y$, so daß wir zwei Arten der Division von B durch A zu unterscheiden haben, die vordere $A^{-1}B$ und die hintere BA^{-1}.

Übungen: 1. Skalare Matrizen sind die einzigen, die mit jeder quadratischen Matrix vertauschbar sind.

2. Man zeige, daß A^{-1} die einzige Matrix ist, die durch vordere (und hintere) Multiplikation mit A die Einheitsmatrix ergibt.

---

1) Ein anderer Beweis folgt aus 1.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

3. Durch Multiplikation der Matrizen

$$E=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad i=\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix},\quad j=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad k=\begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix}$$

zeige man, daß $\qquad i^2=j^2=k^2=-E,\ ij=k,$

und durch Anwendung des assoziativen Gesetzes, daß

$$ik=iij=-j,\ kj=ijj=-i,\ ki=k(-kj)=j,$$
$$ji=kii=-k,\ jk=j(-ji)=i.$$

Jede lineare Kombination von E, i, j, k mit numerischen Koeffizienten heißt eine **Quaternion**. Die beiden Quaternionen

$$q=aE+bi+cj+dk,\quad q'=aE-bi-cj-dk$$

heißen zueinander konjugiert. Man bestätige, daß

$$q=\begin{pmatrix}x&y\\-\bar{y}&\bar{x}\end{pmatrix},\quad q'=\begin{pmatrix}\bar{x}&-y\\\bar{y}&x\end{pmatrix},$$

wo $\qquad x=a+b\sqrt{-1},\quad y=c+d\sqrt{-1},$

und daß $qq'=q'q=nE$, wo $n=x\bar{x}+y\bar{y}$ die Norm von q heißt und mit Nq bezeichnet wird.

4. Die Konjugierte des Produkts zweier Quaternionen ist gleich dem Produkt ihrer in umgekehrter Reihenfolge multiplizierten Konjugierten. Denn es ist für

$$p=\begin{pmatrix}u&v\\-\bar{v}&\bar{u}\end{pmatrix},\quad qp=\begin{pmatrix}r&s\\-\bar{s}&\bar{r}\end{pmatrix},\quad p'q'=\begin{pmatrix}\bar{r}&-s\\\bar{s}&r\end{pmatrix}=(qp)',$$

wo $r=xu-y\bar{v}$, $s=xv+y\bar{u}$. Jetzt ergibt sich die Norm von qp zu

$$qp\cdot p'q'=q\cdot Np\cdot E\cdot q'=qq'\cdot Np\cdot E=Nq\cdot Np\cdot E,$$

d. h. die Norm eines Produkts ist gleich dem Produkt der Normen der Faktoren.

5. In (2) und (6) seien die a_{ij}, b_{ij}, p_{ij} selbst wiederum Matrizen und zwar solche, daß Glieder derselben Zeile jedesmal Matrizen mit derselben Zahl von Zeilen, solche derselben Spalte jedesmal Matrizen mit derselben Zahl von Spalten sind. Man beweise, daß Gleichung (5) auch hier besteht. Man finde ferner die beiden Produkte von (a_{ij}) und (b_{ij}), wenn $b_{ij}=0$ für $i\neq j$ ist.

25. Charakteristische Gleichung. Es sei A eine $n$reihige quadratische Matrix, deren Elemente von λ unabhängig sind, und E die $n$reihige Einheitsmatrix. Dann heißt $A-\lambda E$ die charakteristische Matrix von A; sie wird erhalten, indem man λ von

Digitized by Google Original from UNIVERSITY OF MICHIGAN

jedem Diagonalelement von A subtrahiert. Die charakteristische Determinante von A ist die Determinante von $A - \lambda E$ und ist ein Polynom in λ vom Grade n:

$$(21)\quad \varphi(\lambda) \equiv a_n\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0, \text{ wo } a_n = (-1)^n.$$

Die Gleichung $\varphi(\lambda) = 0$ heißt die charakteristische Gleichung von A.

Z. B. ist die charakteristische Gleichung von

$$(22)\quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}: \varphi(\lambda) = \begin{vmatrix} a-\lambda & b \\ c & d-\lambda \end{vmatrix} = \lambda^2 - (a+d)\lambda + ad - bc.$$

Setzen wir in einem Polynom $f(\lambda) = \Sigma c_i\lambda^i$ an Stelle von λ die Matrix A und multiplizieren c_0 mit E, so erhalten wir eine Matrix, die man mit $f(A)$ bezeichnet. Im Falle (22) bekommen wir so

$$\varphi(A) = A^2 - (a+d)A + (ad - bc)E,$$

was, wie man leicht beweist, gleich Null ist. Dieses Ergebnis ordnet sich dem wichtigen allgemeinen Satz unter:

Satz 4: Jede quadratische Matrix erfüllt ihre charakteristische Gleichung.

Wir haben zu beweisen, daß $\varphi(A) = 0$, wo $\varphi(\lambda)$ die charakteristische Determinante (21) von A bezeichnet. Da die Elemente von $A - \lambda E$ lineare Funktionen von λ und die Elemente ihrer Adjungierten C $(n-1)$reihige Determinanten sind, so sind letztere Polynome in λ von höchstens $n-1$tem Grade. Bezeichnet man daher das Element der $i$ten Zeile $j$ten Spalte von C mit $\sum_k c_{ijk}\lambda^k$ und setzt zur Abkürzung die Matrix

$$(c_{ijk}) = C_k \qquad (i,j = 1,\ldots,n),$$

so ist $$C = \left(\sum_{k=0}^{n-1} c_{ijk}\lambda^k\right) = \sum_{k=0}^{n-1}(c_{ijk})\lambda^k = \sum_{k=0}^{n-1} C_k\lambda^k.$$

Wendet man (16) auf $A - \lambda E$ an, so folgt

$$(A - \lambda E)\cdot C = \varphi(\lambda)\cdot E,$$

d. h. $$A\sum_{k=0}^{n-1} C_k\lambda^k - \lambda\sum_{k=0}^{n-1} C_k\lambda^k = \sum_{k=0}^{n} a_k\lambda^k \cdot E.$$

Setzt man die Koeffizienten der entsprechenden Potenzen von λ auf beiden Seiten einander gleich, so erhält man

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$$\begin{aligned} AC_0 &= a_0E \\ AC_1 - C_0 &= a_1E \\ AC_2 - C_1 &= a_2E \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ AC_{n-1} - C_{n-2} &= a_{n-1}E \\ - C_{n-1} &= a_nE. \end{aligned}$$

Multiplizieren wir diese Gleichungen linksseitig der Reihe nach mit $E, A, A^2, \ldots, A^{n-1}, A^n$ und addieren, so erhalten wir

$$0 = a_0E + a_1A + a_2A^2 + \cdots + a_{n-1}A^{n-1} + a_nA^n \equiv \varphi(A).$$

26. Rang einer Matrix. Jede Matrix M mit mehr als einem Element enthält andere Matrizen, die man aus M durch Tilgung von Zeilen oder Spalten oder Zeilen und Spalten erhält. Insbesondere enthält sie gewisse quadratische Matrizen, deren Determinanten man die Determinanten von M nennt.

Eine Matrix heißt vom Range r, wenn sie mindestens eine nicht verschwindende $r$reihige Determinante enthält, während alle ihre Determinanten von höherer als $r$ter Ordnung verschwinden. Die Nullmatrix, deren Elemente alle gleich Null sind, heißt vom Range Null.

Z. B. ist der Rang der Matrix

$$\begin{pmatrix} a & b & c & d & e \\ p & q & r & s & t \\ a & b & c & d & e \\ p & q & r & s & t \end{pmatrix}$$

gleich 2 oder 1 oder 0, da alle dreireihigen Determinanten verschwinden, und zwar ist der Rang gleich 2, wenn a, b, c, d, e nicht proportional zu p, q, r, s, t sind, so daß jede 2reihige Determinante $\neq 0$ ist; andernfalls ist er gleich 1 oder 0.

Unter dem Rang einer Determinante versteht man den ihrer Matrix.

Satz 5: Wenn A eine Matrix mit n Spalten und B eine solche mit n Zeilen ist, so ist jede t-reihige Determinante D von AB gleich einer Summe von Gliedern, deren jedes das Produkt zweier t-reihigen Determinanten von A und B ist.

Für $n = 3$, $t = 2$ haben wir z. B.

$$\begin{vmatrix} p_{12} p_{13} \\ p_{22} p_{23} \end{vmatrix} = \begin{vmatrix} a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32}, & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32}, & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} a_{12} \\ a_{21} a_{22} \end{vmatrix} \cdot \begin{vmatrix} b_{12} b_{13} \\ b_{22} b_{23} \end{vmatrix} + \begin{vmatrix} a_{11} a_{13} \\ a_{21} a_{23} \end{vmatrix} \cdot \begin{vmatrix} b_{12} b_{13} \\ b_{32} b_{33} \end{vmatrix} + \begin{vmatrix} a_{12} a_{13} \\ a_{22} a_{23} \end{vmatrix} \cdot \begin{vmatrix} b_{22} b_{23} \\ b_{32} b_{33} \end{vmatrix}.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Es sei wie bisher $A = (a_{ij})$, $B = (b_{jk})$, $P = (p_{ik})$. Jede $t$reihige Determinante D von P hat die Form

$$D = \begin{vmatrix} p_{i_1 k_1} & \cdots & p_{i_1 k_t} \\ \cdot & & \cdot \\ p_{i_t k_1} & \cdots & p_{i_t k_t} \end{vmatrix} = \begin{vmatrix} \sum_{j_1=1}^{n} a_{i_1 j_1} b_{j_1 k_1} & \cdots & \sum_{j_t=1}^{n} a_{i_1 j_t} b_{j_t k_t} \\ \cdot & & \cdot \\ \sum_{j_1=1}^{n} a_{i_t j_1} b_{j_1 k_1} & \cdots & \sum_{j_t=1}^{n} a_{i_t j_t} b_{j_t k_t} \end{vmatrix},$$

wo $i_1 < i_2 < \cdots < i_t$, $k_1 < k_2 < \cdots < k_t$. Da jedes Element der ersten Spalte eine Summe von n Gliedern ist, so ist D gleich der Summe von n Determinanten, deren $j_1$te als Elemente der ersten Spalte die $j_1$ten Glieder dieser Summen und als Elemente der übrigen Spalten die Elemente von D besitzt. Mit anderen Worten: wir können das Summationszeichen aus der ersten Spalte entfernen und vor die Determinante setzen, ebenso den gemeinsamen Faktor $b_{j_1 k_1}$. Ähnlich verfährt man bei den übrigen Spalten und erhält

$$D = \sum_{j_1=1}^{n} \cdots \sum_{j_t=1}^{n} \Delta \cdot b_{j_1 k_1} \cdots b_{j_t k_t},$$

wo

$$\Delta = \begin{vmatrix} a_{i_1 j_1} & \cdots & a_{i_1 j_t} \\ \cdot & & \cdot \\ a_{i_t j_1} & \cdots & a_{i_t j_t} \end{vmatrix}.$$

Wenn nun unter den Zahlen $j_1, \ldots j_t$ gleiche vorkommen, so ist $\Delta = 0$. Im anderen Fall ist $j_1, \ldots, j_t$ immer eine Anordnung von t aus $1, \ldots, n$ herausgegriffenen Zahlen. Ist diese Anordnung natürlich, d. h. steht keine kleinere Zahl hinter einer größeren, so ist Δ selbst eine $t$reihige Determinante α von A. Ist die Anordnung nicht natürlich, so möge sie durch l sukzessive Vertauschungen je zweier Zahlen in eine natürliche übergehen. Dann geht aber auch Δ durch l entsprechende Vertauschungen je zweier Spalten in ein α über, so daß $\Delta = (-1)^l \cdot \alpha$ ist. Die Summe aller so in D entstehenden $t!$ Produkte $(-1)^l b_{j_1 k_1} \ldots b_{j_t k_t}$ ist aber nichts anderes als die Determinante

$$\beta = \begin{vmatrix} b_{g_1 k_1} & \cdots & b_{g_1 k_t} \\ \cdot & & \cdot \\ b_{g_t k_1} & \cdots & b_{g_t k_t} \end{vmatrix}$$

von B ($g_1, \ldots, g_t$ ist die natürliche Anordnung von $j_1, \ldots, j_t$). Daher ist $D = \Sigma \alpha \beta$, wo die Summe über alle erwähnten natürlichen Anordnungen zu erstrecken ist.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Folgerung: Der Rang des Produkts zweier Matrizen kann nie den Rang eines der Faktoren übersteigen.

Denn wenn alle $t$reihigen Determinanten von A (oder B) gleich Null sind, so sind es auch alle $t$reihigen Determinanten von AB.

Satz 6: Wenn A eine mn-Matrix und B eine nicht-singuläre n-reihige quadratische Matrix ist, so haben A und AB denselben Rang. Ist ferner C eine nicht-singuläre m-reihige quadratische Matrix, so haben A und CA denselben Rang.

Denn wenn r der Rang von A und ϱ der von $P = AB$ ist, so ist nach Obigem $\varrho \leqq r$ und für $A = PB^{-1}$ ist $r \leqq \varrho$, also $r = \varrho$. Ähnlich verläuft der Beweis für den anderen Fall.

27. Bilineare Formen. Ein Polynom in den $m + n$ Variabeln $x_1, \ldots, x_m, y_1, \ldots, y_n$ heißt eine bilineare Form, wenn jedes seiner Glieder linear in den x und linear in den y ist. Ein Beispiel für $m = 1$, $n = 2$ wäre etwa $7x_1y_1 - 5x_1y_2$. Die allgemeine bilineare Form ist

$$\alpha = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j. \tag{23}$$

Schreiben wir $\alpha = \sum_{i=1}^{m} x_i l_i$, wo $l_i = \sum_{j=1}^{n} a_{ij} y_j$ $(i = 1, \ldots, m)$,

so heißt die Matrix $A = (a_{ij})$ dieser m linearen Formen l_i die Matrix der bilinearen Form (23).

Nach Satz 1 ersetzt die lineare Transformation (7) mit der Matrix B l_i durch $\sum_k p_{ik} z_k$, wo $(p_{ik}) = AB$ ist, d. h. sie ersetzt α durch die Form

$$\sum_{i=1}^{m} \sum_{k=1}^{n} p_{ik} x_i z_k$$

mit der Matrix AB.

Ändern wir nicht die y, sondern die x durch die Transformation

$$x_i = \sum_{k=1}^{m} c_{ik} \xi_k \qquad (i = 1, \ldots, m) \tag{24}$$

mit der Matrix C, so geht α aus (23) über in

$$\sum_{i,k=1}^{m} \sum_{j=1}^{n} c_{ik} a_{ij} \xi_k y_j = \sum_{k=1}^{m} \sum_{j=1}^{n} d_{kj} \xi_k y_j,$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

wo $d_{kj} = \Sigma_i c_{ik} a_{ij}$. d_{kj} ist aber die Summe der Produkte der Elemente der $k$ten Zeile der Matrix

$$C' = \begin{pmatrix} c_{11} \cdots c_{m1} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ c_{1m} \cdots c_{mm} \end{pmatrix}$$

und der entsprechenden Elemente der $j$ten Spalte von $A = (a_{ij})$, so daß die neue bilineare Form die Matrix $C'A$ hat. C' heißt die Transponierte der Matrix C; man erhält sie aus C durch „Stürzen", d. h. durch Vertauschen von Zeilen mit Spalten oder durch Schwenken um die Hauptdiagonale.

Satz 7: Wenn wir in einer bilinearen Form mit der Matrix A die x einer linearen Transformation (24) mit der Matrix C und die y einer linearen Transformation mit der Matrix B unterwerfen, so erhalten wir eine neue bilineare Form mit der Matrix $C'AB$, wo C' Transponierte von C ist.

Schreiben wir die bilineare Form (23) in der Gestalt

$$\alpha = \sum_{j=1}^{n} \lambda_j y_j, \quad \text{wo} \quad \lambda_j = \sum_{i=1}^{m} a_{ij} x_i \qquad (j = 1, \ldots, n),$$

so ist die Matrix der linearen Formen $\lambda_1, \ldots, \lambda_n$ die Transponierte A' von A. Die Transformation (24) mit der Matrix C ersetzt $\lambda_1, \ldots, \lambda_n$ durch lineare Funktionen von $\xi_1, \ldots, \xi_m$, deren Koeffizientenmatrix nach Satz 1 gleich $A'C$ ist, d. h. sie ersetzt α durch eine bilineare Form mit der Matrix $(A'C)'$, welche aber nach dem unserem Satz (7) vorausgehenden Ergebnis gleich $C'A$ ist. Da A die Transponierte von A' ist, so haben wir

Satz 8: Die Transponierte eines Produktes von Matrizen erhält man, indem man die Transponierten der Faktoren bildet und diese dann in umgekehrter Reihenfolge miteinander multipliziert.

Übungen: 1. Beweise Satz 8 durch direkte Multiplikation.

2. Beweise mittels der Transponierten von $AA^{-1} = E$, daß $(A')^{-1} = (A^{-1})'$.

3. Wenn $AA' = E$, ist auch $A'A = E$.

4. Eine mn-Matrix (a_{ij}) ist dann und nur dann vom Rang 0 oder 1, wenn $m + n$ Zahlen $c_1, \ldots, c_m$, $d_1, \ldots, d_n$ existieren, so daß $a_{ij} = c_i d_j$ $(i = 1, \ldots, m;\ j = 1, \ldots, n)$.

28. Körper. Zwei Formen (die beide linear, bilinear oder quadratisch sind) können gegenüber einer Transformation mit komplexen Koeffizienten äquivalent sein, ohne es gegenüber einer

Digitized by Google Original from UNIVERSITY OF MICHIGAN

reellen Transformation zu sein. Dasselbe gilt für zwei Formen gegenüber zwei Transformationen, von denen die eine reelle, die andere rationale Koeffizienten hat. Hier wie anderwärts in der neueren Algebra ist es daher nötig, die Natur der verwendeten Konstanten genau anzugeben. Um diese kurz und klar auszudrücken und um unseren Sätzen volle Allgemeinheit zu geben, benutzen wir den Begriff des „Körpers" oder „(Rationalitäts-) Bereiches".

Ein System komplexer Zahlen $a + bi$ heißt ein Körper, wenn Summe, Differenz, Produkt und Quotient (die Division durch Null bleibt ausgeschlossen) irgend zweier Zahlen des Systems wiederum in dem System vorkommen.[1])

So bilden z. B. folgende Zahlensysteme jedesmal einen Körper: alle komplexen Zahlen; alle reellen Zahlen; alle rationalen Zahlen; alle Zahlen der Form $a + br$, wo a und b rational sind und $r = i$ oder $r = \sqrt{3}$ ist.

Hingegen ist das System aller ganzen Zahlen kein Körper; ebensowenig alle positiven reellen (oder rationalen) Zahlen.

29. Lineare Unabhängigkeit.[2]) Die Größen (Zahlen oder Funktionen), $l_1, \ldots, l_n$ heißen linear abhängig in bezug auf den Körper K, wenn es in K Zahlen $c_1, \ldots, c_n$ (die nicht alle verschwinden) gibt, so daß

$$c_1 l_1 + \cdots + c_n l_n = 0. \tag{25}$$

Wenn keine solchen Zahlen c_i existieren, so heißen $l_1, \ldots, l_n$ linear unabhängig in K.

Wir gebrauchen diese Terminologie auch noch im Falle $n = 1$, wo wir also von „Abhängigkeit" eigentlich nicht reden können. Wir nennen aber trotzdem l_1 linear abhängig oder nicht, je nachdem $l_1 = 0$ oder $l_1 \neq 0$.

---

1) Ausgedehnte Anwendungen des Körperbegriffes enthält z. B. die Theorie der höheren komplexen Zahlen, worüber man das Buch des Verfassers „Algebras and Their Arithmetics", Univers. of Chicago Press. (Deutsche Ausgabe „Algebren und ihre Zahlentheorie", Orell Füssli, Zürich 1927) vergleichen möge.

2) Wir werden die Theorie der linearen Gleichungssysteme, deren Koeffizienten irgendeinem Körper angehören, nicht voraussetzen, sondern sie in §§ 31, 32 aus der gegenwärtigen Untersuchung gewinnen. Daher vermeiden wir den kürzeren Beweis von Satz 9, der mit Hilfe dieser Theorie möglich wäre.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 9: Wenn $y_1, \ldots, y_n$ linear unabhängig in K sind, dann sind die n linearen Funktionen

$$l_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, n) \tag{26}$$

mit Koeffizienten aus K linear unabhängig oder nicht in K, je nachdem die Determinante $\Delta = |a_{ij}| \neq 0$ oder $= 0$.

Es sei zunächst $\Delta \neq 0$. Man nehme an, es bestehe eine Beziehung von der Art (25). Dann folgt aus

$$\sum_{i=1}^{n} c_i l_i \equiv \sum_{i,j=1}^{n} c_i a_{ij} y_j = 0,$$

daß wegen der linearen Unabhängigkeit alle Koeffizienten der y verschwinden, d. h. daß

$$\sum_{i=1}^{n} a_{ij} c_i = 0$$

für $j = 1, \ldots, n$. Löst man diese Gleichungen nach den c auf, so erhält man $\Delta \cdot c_i = 0$, also alle $c_i = 0$ gegen die Voraussetzung.

Wenn umgekehrt $l_1, \ldots, l_n$ unabhängig sind, so ist $\Delta \neq 0$. Um dies zu beweisen, wenden wir den Schluß von n auf $n+1$ an, indem wir bemerken, daß der Satz für $n = 1$ selbstverständlich ist. Zunächst kann kein l gleich Null sein, denn wenn $l_n = 0$ wäre, so wäre $1 \cdot l_n = 0$ eine Abhängigkeitsbeziehung (25). Durch Umbenennung der y können wir dann immer erreichen, daß $a_{nn} \neq 0$. Da ferner unser Satz bewiesen ist, wenn er für $l_1, \ldots, l_{n-1}$, $a_{nn}^{-1} l_n$ gilt, so dürfen wir $a_{nn} = 1$ annehmen.

Dann sind $$z_i = l_i - a_{in} l_n = \sum_{j=1}^{n-1} (a_{ij} - a_{in} a_{nj}) y_j \qquad (i = 1, \ldots, n-1)$$

linear unabhängige Funktionen von $y_1, \ldots, y_{n-1}$, da aus

$$\sum_{i=1}^{n-1} c_i z_i = \sum_{i=1}^{n-1} c_i (l_i - a_{in} l_n) = 0$$

wegen der linearen Unabhängigkeit der $l_1, \ldots, l_n$ folgen würde, daß jedes $c_i = 0$ wäre.

Da unser Satz nach Voraussetzung für $n - 1$ gilt, so ist die Determinante der z_i

$$D = |a_{ij} - a_{in} a_{nj}| \neq 0 \qquad (i, j = 1, \ldots, n-1).$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Subtrahieren wir jetzt in Δ von der 1ten, 2ten, ..., $n-1$ten Spalte die mit $a_{n1}, a_{n2}, \ldots, a_{n,n-1}$ nacheinander multiplizierte letzte Spalte, so erhalten wir eine Determinante, deren letzte Zeile 0, 0, ..., 0, 1 ist und welche D als Unterdeterminante von 1 hat. Daher ist $\Delta = D \neq 0$.

Satz 10: Wenn $y_1, \ldots, y_n$ in K linear unabhängig und $l_1, \ldots, l_m$ lineare Formen in $y_1, \ldots, y_n$ mit Koeffizienten aus K sind, so können wir gewisse der l, etwa

$$\eta_i = l_{k_i} \qquad (i = 1, \ldots, r)$$

auswählen, welche in K linear unabhängig und so beschaffen sind, daß die $m - r$ übrig bleibenden l linear durch $\eta_1, \ldots, \eta_r$ mit Koeffizienten aus K ausdrückbar sind.

Als η_1 können wir jedes in den y nicht identisch verschwindende l_{k_1} nehmen. Wenn jedes l_j das Produkt von η_1 und einer Zahl aus K ist, so ist der Satz richtig (es ist dann $r = 1$). Andernfalls wählen wir irgendein l_{k_2}, welches nicht ein solches Produkt ist, als η_2, so daß also η_1 und η_2 unabhängig sind. Ist jedes l_j jetzt eine lineare Kombination von η_1 und η_2 mit Koeffizienten aus K, so ist der Satz richtig (es ist $r = 2$). Anderenfalls wähle man als η_3 ein l_{k_3}, welches keine solche lineare Kombination ist usw.

Der Wert von r folgt aus Satz 13.

Satz 11: Wenn in Satz 10 $r < n$ ist, so existieren lineare Formen $\eta_{r+1}, \ldots, \eta_n$ in $y_1, \ldots, y_n$ mit Koeffizienten aus K, so daß $\eta_1, \ldots, \eta_n$ in K linear unabhängig sind.

Zunächst sind zwar die η lineare Funktionen der y, hingegen sind nicht umgekehrt alle $y_1, \ldots, y_n$ lineare Funktionen von $\eta_1, \ldots, \eta_r$ mit Koeffizienten aus K. Denn sonst wäre insbesondere

$$y_i = \sum_{k=1}^{r} t_{ik} \eta_k \qquad (i = 1, \ldots, r) \tag{27}$$

und daher nach Satz 9 $|t_{ik}| \neq 0$. Die Gleichungen (27) ließen sich also auflösen und drückten die η_k als lineare Funktionen der $y_1, \ldots, y_r$ mit Koeffizienten aus K aus. Nach Voraussetzung ist nun $y_i (i > r)$ eine lineare Funktion der η und daher auch der $y_1, \ldots, y_r$ mit Koeffizienten aus K. Dies widerspricht aber der Unabhängigkeit der y.

Daher sind auch nicht alle linearen Funktionen von $y_1, \ldots, y_n$ mit Koeffizienten aus K lineare Funktionen von $\eta_1, \ldots, \eta_r$ mit

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Koeffizienten aus K. Infolgedessen gibt es eine lineare Funktion η_{r+1} der y, so daß $\eta_1, \ldots, \eta_r, \eta_{r+1}$ linear unabhängig in K sind. Ist nun $r+1=n$, so ist der Satz bewiesen. Ist $r+1<n$, so wiederholen wir den Schluß so oft, bis wir n erreichen.

30. Äquivalenz zweier Matrizen bzw. bilinearer Formen. Zwei bilineare Formen α und α_1 in $x_1, \ldots, x_m, y_1, \ldots, y_n$ mit Koeffizienten aus K heißen dann und nur dann in K äquivalent, wenn α in α_1 übergeht, wenn wir die x einer gewissen linearen nichtsingulären Transformation C und die y einer gewissen nichtsingulären linearen Transformation B unterwerfen (wobei die Elemente von B und C die K enthalten sind). In diesem Fall heißen auch die Matrizen A und A_1 von α und α_1 in K äquivalent. Nach Satz 7 ist dann $A_1 = C'AB$. Mit anderen Worten: Zwei mn-Matrizen A und A_1 mit Elementen aus K heißen dann und nur dann in K äquivalent, wenn es zwei nichtsinguläre quadratische Matrizen[1]) D und B mit m bzw. n Reihen und mit Elementen aus K gibt, so daß $DAB = A_1$.

Satz 12: Zwei Matrizen (oder bilineare Formen) in K sind dann und nur dann in K äquivalent, wenn sie denselben Rang haben.

Sind die Matrizen äquivalent, so haben sie nach Satz 6 denselben Rang. Sind umgekehrt α und α_1 bilineare Formen in K mit demselben Rang, so sind sie äquivalent in K. Bei dem Rang Null, wo $\alpha \equiv 0$, $\alpha_1 \equiv 0$, ist dies selbstverständlich. Allgemein werden wir den Satz so beweisen, daß wir jede der beiden Formen in eine Normalform transformieren. Von letzteren ist dann der Satz leichter zu beweisen.

Wir gehen aus von der bilinearen Form α

$$\alpha = \sum_{i=1}^{m} x_i l_i, \quad l_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, m),$$

in welcher die a_{ij} Zahlen aus K sind, die nicht alle verschwinden. Nach Satz 10 können wir gewisse der l, etwa $\eta_i = l_{k_i}$ $(i = 1, \ldots, r)$, die in K linear unabhängig sind, auswählen, so daß die $m-r$ übrigbleibenden l lineare Funktionen der $\eta_1, \ldots, \eta_r$ mit Koeffizienten aus K sind. Da ferner $k_1, \ldots, k_r$ verschieden sind, so können wir $m-r$ weitere k hinzunehmen, so daß dann $k_1, \ldots,$

1) Wir haben hier D an Stelle von C' geschrieben. Umgekehrt bekommen wir bei gegebenem D das C als D'.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$k_r, \ldots, k_m$ eine Permutation von $1, \ldots, m$ bilden. Bezeichnet man l_{k_i} auch für $i > r$ mit η_i und führt die neuen Variabeln

$$X_i = x_{k_i} \qquad (i = 1, \ldots, m)$$

ein, so ist

$$\alpha = \sum_{i=1}^{m} x_{k_i} l_{k_i} = \sum_{i=1}^{m} X_i \eta_i,$$

wo für $i = r + 1, \ldots, m$

$$\eta_i = \sum_{j=1}^{r} d_{ij} \eta_j$$

ist und die d_{ij} zu K gehören, d. h. es ist

$$\alpha = \sum_{j=1}^{r} X_j \eta_j + \sum_{i=r+1}^{m} X_i \sum_{j=1}^{r} d_{ij} \eta_j = \sum_{j=1}^{r} \xi_j \eta_j,$$

wenn wir zur Abkürzung

$$\xi_j = X_j + \sum_{i=r+1}^{m} d_{ij} X_i \qquad (j = 1, \ldots, r)$$

setzen. Letztere und $\xi_i = X_i$ $(i = r + 1, \ldots, m)$ geben m linear unabhängige Funktionen $\xi_1, \ldots, \xi_m$ von $X_1, \ldots, X_m$ und daher auch von $x_1, \ldots, x_m$ mit Koeffizienten aus K. Nach Satz 9 ist daher die Determinante der Matrix M der Koeffizienten von $x_1, \ldots, x_m$ von Null verschieden. Ist nun $r < n$, so gibt es nach Satz 11 lineare Funktionen $\zeta_{r+1}, \ldots, \zeta_n$ von $y_1, \ldots, y_n$ mit Koeffizienten aus K, so daß $\eta_1, \ldots, \eta_r, \zeta_{r+1}, \ldots, \zeta_n$ linear unabhängig in K sind. Ist aber $r = n$, so unterdrücken wir die ζ und gebrauchen nur $\eta_1, \ldots, \eta_n$. In beiden Fällen ist die Determinante der Matrix N der Koeffizienten der $y_1, \ldots, y_n$ in diesen n linearen Funktionen nach Satz 9 von Null verschieden.

Damit haben wir unsere gewünschte Normalform erhalten: Durch eine lineare Transformation der x, welche die x als lineare Funktionen der ξ mit der Matrix M^{-1} ausdrückt, und durch eine lineare Transformation der y mit der Matrix N^{-1}, welche die y linear durch die η und ζ ausdrückt, können wir α auf die Form

$$\sum_{j=1}^{r} \xi_j \eta_j \tag{28}$$

bringen. Die Matrix von (28) hat offenbar den Rang r. Nach dem ersten Teil unseres Satzes ist daher auch α vom Range r, und da α

Digitized by Google Original from UNIVERSITY OF MICHIGAN

und α_1 beide äquivalent zu (28) sind, so sind sie auch einander äquivalent.

Wir haben damit gleichzeitig schon den ersten Teil des Satzes bewiesen:

Satz 13: Die in Satz 10 vorkommende Zahl r ist der Rang der Matrix der Koeffizienten von $l_1, \ldots, l_m$. Ebenso ist auch der Rang der Matrix T der Koeffizienten von $\eta_1, \ldots, \eta_r$ gleich r.

Ist nämlich der Rang ϱ von T kleiner als r, so sind nach dem ersten Teil des Satzes $r - \varrho$ der η linear durch ϱ derselben mit Koeffizienten aus K ausdrückbar, im Widerspruch mit der linearen Unabhängigkeit der $\eta_1, \ldots, \eta_r$ in K.

Folgerung 1: Für $m > n$ sind m beliebige lineare Formen in n unabhängigen Variabeln mit Koeffizienten aus K linear abhängig in K.

Denn der Rang r ist offenbar $\leqq n$ und daher $< m$. Dann lassen sich nach Satz 10 $m - r$ der Formen durch r von ihnen ausdrücken, so daß die m Formen abhängig sind.

Da umgekehrt bei linearer Abhängigkeit der m Formen ihr Rang $r < m$ ist, so gilt

Folgerung 2: m beliebige lineare Formen in n unabhängigen Variabeln mit Koeffizienten aus K sind dann und nur dann in K abhängig, wenn jede $m$reihige Determinante der Koeffizientenmatrix verschwindet.

Übungen: 1. Man finde die linearen Transformationen, die $2x_1y_2 - 3x_1y_3 + 4x_2y_1 - 2x_2y_3 - 3x_3y_1 + x_3y_2$ in $\xi_1\eta_1 + \xi_2\eta_2$ überführen.

2. $5x + 3y - 6, 8x + 15z, 6x + 2y + 5z - 4$ sind linear abhängig.

3. Wiederhole Satz 12 für den Körper der reellen Zahlen, ohne den Begriff des Körpers explizite zu gebrauchen.

4. Jede Matrix vom Range r ist einer Matrix äquivalent, in der $a_{ii} = 1$, wenn $i \leqq r$, und in der alle übrigen Elemente verschwinden.

5. Jede Matrix vom Range r läßt sich als Summe von r Matrizen vom Range 1 darstellen. Daher kann jede bilineare Form vom Range r als Summe von r Produkten dargestellt werden, wobei der eine Faktor jedesmal eine lineare Form in $x_1, \ldots, x_m$ und der andere eine lineare Form in $y_1, \ldots, y_n$ ist.

6. Wenn eine bilineare Form die Summe von r Gliedern ist, deren jedes das Produkt einer linearen Form in $x_1, \ldots, x_m$ und einer linearen Form in $y_1, \ldots, y_n$ ist, so hat die Matrix der Form dann und nur dann den Rang r, wenn die r linearen Formen in den x und die r Formen in den y linear unabhängig sind.

7. Ist r der Rang einer $n$reihigen quadratischen Matrix und R der Rang der aus ihren t ersten Zeilen gebildeten Matrix, so ist $R \geqq r + t - n$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

8. Wenn r_1 und r_2 die Rangzahlen zweier $n$reihigen quadratischen Matrizen sind und wenn R der Rang ihres Produktes ist, so zeige mann, daß $R \geqq r_1 + r_2 - n$. Anleitung: Beweise die Tatsache zuerst für den Fall, daß der linke Faktor die Form von Beispiel 4 hat.

31. **Homogene lineare Gleichungen.** Wir gehen aus von einem System von Gleichungen $l_1 = 0, \ldots, l_m = 0$ in den Unbekannten $y_1, \ldots, y_n$ mit Koeffizienten aus K und mit dem Rang r. Nach Umordnen der Gleichungen können wir wegen Satz 13 voraussetzen, daß $l_1, \ldots, l_r$ linear unabhängig sind und eine Matrix M vom Range r haben, während $l_{r+1}, \ldots, l_m$ lineare Kombinationen von $l_1, \ldots, l_r$ mit Koeffizienten aus K sind. Mindestens eine $r$reihige Determinante von M ist von Null verschieden und nach Umbenennen der y können wir voraussetzen, daß dies die Determinante D der Koeffizienten von $y_1, \ldots, y_r$ in $l_1 = 0, \ldots, l_r = 0$ ist. Man schaffe die Glieder mit y_j $(j > r)$ auf die andere Seite und wende die gewöhnliche Determinantenmethode an. Dann erhalten wir

$$y_i = \sum_{j=r+1}^{n} c_{ij} y_j \qquad (i = 1, \ldots, r) \tag{29}$$

wo die c_{ij} zu K gehören, und durch Einsetzen dieser Werte von $y_1, \ldots, y_r$ in $l_1, \ldots, l_r$ erhalten wir daher Ausdrücke in $y_{r+1}, \ldots, y_n$, die für alle Werte der letzteren gleich Null sind. Dasselbe ist für $l_{r+1}, \ldots, l_m$ der Fall, da sie lineare Kombinationen von $l_1, \ldots, l_r$ sind.

Satz 14: Aus m homogenen linearen Gleichungen in n Unbekannten, deren Koeffizienten zu einem Körper K gehören und eine Matrix vom Range r besitzen, lassen sich r Gleichungen mit nichtverschwindender Determinante auswählen, durch welche r der Unbekannten sich eindeutig als homogene lineare Funktionen (mit Koeffizienten aus K) der n — r übrigbleibenden Unbekannten ausdrücken lassen. Diese Werte für die r Unbekannten erfüllen die m gegebenen Gleichungen identisch, d. h. bei beliebigen Werten jener n — r Unbekannten.

Folgerung: Es existieren dann und nur dann wesentliche Lösungen (d. h. Lösungen, die nicht alle gleich Null sind), wenn $r < n$, d. h. erst recht, wenn $m < n$. **Insbesondere haben n homogene lineare Gleichungen in n Unbekannten dann und nur dann wesentliche Lösungen, wenn ihre zugehörige Determinante verschwindet.**

Wenn die homogenen linearen Gleichungen $l_1 = 0, \ldots, l_m = 0$ die beiden Lösungen $(u_1, \ldots, u_n)$ und $(v_1, \ldots, v_n)$ besitzen, so

Digitized by Google Original from UNIVERSITY OF MICHIGAN

haben sie offenbar die allgemeine Lösung $(gu_1 + hv_1, \ldots, gu_n + hv_n)$, in der g und h irgendwelche Zahlen sind. Wir nennen ähnlich wie bisher die beiden Lösungen **linear abhängig**, wenn es Konstanten g und h, die nicht beide gleich Null sind, gibt, so daß $gu_i + hv_i = 0$ $(i = 1, \ldots, n)$, hingegen **linear unabhängig**, wenn keine solchen Konstanten g und h existieren. Analoge Definitionen gelten für mehr als zwei Lösungen.

Z. B. hat die Gleichung $2y_1 + 3y_2 - 5y_3 = 0$ die unabhängigen Lösungen

$$(u_1, u_2, u_3) = (-\tfrac{3}{2}, 1, 0); \quad (v_1, v_2, v_3) = (\tfrac{5}{2}, 0, 1),$$

während jede andere Lösung (y_1, y_2, y_3) sich aus ihnen zusammen setzt:

$$y_1 = gu_1 + hv_1, \quad y_2 = gu_2 + hv_2, \quad y_3 = gu_3 + hv_3.$$

Dieses Beispiel erläutert den Satz:

Satz 15: Jedes System von m homogenen linearen Gleichungen in $y_1, \ldots, y_n$ vom Rang $r < n$ hat $n - r$ linear unabhängige Lösungen, aus denen sich jede andere Lösung linear zusammensetzt.

Benutzen wir die Bezeichnungen von (29), so können wir als die $n - r$ Lösungen

$$(30) \qquad (c_{1j}, \ldots, c_{rj}, 0, \ldots, 0, 1, 0, \ldots, 0) \qquad (j = r+1, \ldots, n)$$

annehmen, wobei an der $j$ten Stelle die Zahl 1 steht. Nach Multiplikation dieser Lösungen mit y_j und Summierung über j erhalten wir wegen (29) die Lösung

$$\left(\sum y_j c_{1j} = y_1, \ldots, \quad \sum y_j c_{rj} = y_r, \; y_{r+1}, \ldots, y_n\right),$$

in denen von $j = r + 1$ bis $j = n$ summiert wird. Da alle diese Zahlen dann und nur dann verschwinden, wenn $y_{r+1}, \ldots, y_n$ alle gleich Null sind, so sind die Lösungen (30) linear unabhängig.

32. Inhomogene lineare Gleichungen. Es liege ein System von m Gleichungen $l_1 = k_1, \ldots, l_m = k_m$ vor, wo die k Konstanten und die l lineare Formen in $y_1, \ldots, y_n$ bedeuten, deren Matrix A den Rang r besitzt. Nach Umordnungen der Gleichungen können wir erreichen, daß $l_1, \ldots, l_r$ die linear unabhängigen Formen sind, so daß also auch

$$(31) \qquad l_i = \sum_{j=1}^{r} c_{ij} l_j \qquad (i = r+1, \ldots, m).$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Daher sind unsere m Gleichungen $l_i = k_i$ nur dann einander nicht widersprechend, wenn

$$k_i = \sum_{j=1}^{r} c_{ij} k_j \qquad (i = r+1, \ldots, m) \tag{32}$$

Setzt man $\lambda_i \equiv l_i - k_i y_{n+1}$, wo $y_{n+1} = 1$, so sind $\lambda_1, \ldots, \lambda_r$ voneinander unabhängig, da es auch $l_1, \ldots, l_r$ sind.

Hingegen ist

$$\lambda_i = \sum_{j=1}^{r} c_{ij} \lambda_j \qquad (i = r+1, \ldots, m)$$

dann und nur dann, wenn die Bedingungen (32) bestehen, und dann ist nach Satz 13 die Matrix von $\lambda_1, \ldots, \lambda_m$ auch vom Range r.

Satz 16: Es sei r der Rang der Matrix A der homogenen linearen Funktionen $l_1, \ldots, l_m$ von $y_1, \ldots, y_n$. Ferner sei B die Matrix, die aus A durch Hinzufügen einer Kolonne mit den Elementen $k_1, \ldots, k_m$ hervorgeht, so daß der Rang ϱ von $B \geqq r$ ist. Dann stehen die Gleichungen $l_1 = k_1, \ldots, l_m = k_m$ miteinander in Widerspruch, wenn $\varrho > r$. Für $\varrho = r$ jedoch lassen sich r Unbekannte eindeutig durch gewisse r der Gleichungen als lineare Funktionen der $n - r$ übrig bleibenden Unbekannten bestimmen; für beliebige Werte der letzteren sind auch die übrig bleibenden $m - r$ Gleichungen durch die für jene r Unbekannten erhaltenen Ausdrücke erfüllt.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

VIERTES KAPITEL.

QUADRATISCHE UND HERMITESCHE FORMEN. SYMMETRISCHE UND HERMITESCHE BILINEARE FORMEN.

Wir behandeln diese vier Formentypen zusammen, weil dies nur wenig mehr Raum und Mühe erfordert als etwa eine Diskussion der quadratischen Formen allein. Die Wichtigkeit der Hermiteschen Formen in der Metrik usw. tritt immer mehr hervor. — Betreffs der quadratischen Formen müssen wir uns auf das Wesentlichste beschränken, doch genügen auch unsere Ergebnisse zu ihrer metrischen und projektiven Klassifikation.

33. Symmetrische bilineare Formen; quadratische Formen. Die bilineare Form

$$\alpha = \sum_{i,k=1}^{n} a_{ik} x_i y_k \tag{1}$$

heißt symmetrisch, wenn sie bei Vertauschung von x_i und y_i $(i = 1, \ldots, n)$ in sich selbst übergeht; dazu ist offenbar notwendig und hinreichend, daß

$$a_{ik} = a_{ki} \qquad (i,k = 1, \ldots, n). \tag{2}$$

Die zugehörige Matrix $A = (a_{ik})$, die offenbar durch Vertauschung von Reihen und Spalten ungeändert bleibt, heißt ebenfalls symmetrisch; sie ist gleich ihrer transponierten A'.

Nach Kap. III, Satz 7 geht α vermittels der Transformation

$$x_i = \sum_{k=1}^{n} b_{ik} X_k \qquad (i = 1, \ldots, n) \tag{3}$$

mit der Matrix $B = (b_{ik})$ und der kogredienten Transformation

$$y_i = \sum_{k=1}^{n} b_{ik} Y_k \qquad (i = 1, \ldots, n) \tag{4}$$

mit derselben Matrix B in eine bilineare Form α_1 über mit der Matrix $A_1 = B'AB$. Da nun $A' = A$ ist, so ist nach Kap. III, Satz 8 $A_1' = B'A'B = A_1$, d. h. A_1 ist wieder symmetrisch.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Nennt man jetzt zwei $n$reihige quadratische Matrizen A und A_1, deren Elemente in einem Körper K liegen, in K kongruent, wenn es eine nicht singuläre $n$reihige quadratische Matrix B mit Elementen aus K gibt, so daß $A_1 = B'AB$, so erhalten wir unter Benutzung unseres Äquivalentbegriffes von 30. den

Satz 1: Zwei symmetrische bilineare Formen mit Koeffizienten aus einem Körper K sind dann und nur dann gegenüber nichtsingulären kogredienten Transformationen (3) und (4) mit Koeffizienten aus K einander äquivalent, wenn ihre Matrizen in K kongruent sind.

Lassen wir alle y_i mit x_i zusammenfallen, so wird aus der symmetrischen bilinearen Form (1) eine quadratische Form

$$q = \sum_{i,k=1}^{n} a_{ik} x_i x_k, \quad \text{wo} \quad a_{ik} = a_{ki}, \tag{5}$$

mit derselben symmetrischen Matrix $A = A'$. So ist z. B. für $n = 2$

$$q = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2.$$

Rang und Determinante von A heißen jetzt Rang und Determinante von q.

Setzen wir auch in (4) $y_i = x_i$, $Y_k = X_k$, so daß (4) mit (3) identisch wird, so sehen wir, daß die Transformation (3) mit der Matrix B die quadratische Form (5) mit der symmetrischen Matrix A in eine quadratische Form mit der symmetrischen Matrix $B'AB$ überführt; kurz:

Satz 2: Zwei quadratische Formen mit Koeffizienten in einem Körper K sind dann und nur dann äquivalent gegenüber nichtsingulären Transformationen mit Koeffizienten aus K, wenn ihre Matrizen in K kongruent sind.

Vergleicht man Satz 1 und 2, so ergibt sich

Folgerung 1: Zwei symmetrische bilineare Formen mit den Matrizen A und A_1 sind dann und nur dann äquivalent gegenüber kogredienten Transformationen, wenn die entsprechenden quadratischen Formen mit den Matrizen A und A_1 es sind. (Es ist wohl selbstverständlich, daß die Formen und die Äquivalenz sich auf K beziehen.)

Die beiden Äquivalenzprobleme sind also im wesentlichen identisch; beide erfordern eine Untersuchung über die Kongruenz symmetrischer Matrizen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

34. Hermitesche Formen. Hermitesche bilineare Formen. Der Körper S enthalte eine Zahl v, welche nicht das Quadrat einer anderen Zahl aus S ist. Durch Adjunktion von $\sqrt{v}$ zu S erhält man dann einen erweiterten Körper K, der alle Zahlen der Form $x = a + b\sqrt{v}$, wo a und b zu S gehören, enthält. $\bar{x} = a - b\sqrt{v}$ heißt die Konjugierte von x.

Ein wichtiges Beispiel erhält man, wenn man S als den Körper aller reellen Zahlen und $v = -1$ annimmt. Dann ist K der Körper aller komplexen Zahlen, und x und $\bar{x}$ sind konjugiert imaginär.

Die bilineare Form mit Koeffizienten aus K

$$\sum_{i,k=1}^{n} a_{ik} x_i y_k, \quad \text{wo} \quad a_{ik} = \bar{a}_{ki}, \tag{6}$$

heißt eine Hermitesche bilineare Form in K.

Ersetzen wir jedes Element der Matrix A durch sein konjugiertes, so erhalten wir die zu A konjugierte Matrix $\bar{A}$. Offenbar gelten die Regeln

$$\bar{\bar{M}} = M, \quad \overline{MN} = \bar{M}\bar{N}, \quad (\bar{M})' = \overline{M'}. \tag{7}$$

Die Matrix A von (6) mit der Eigenschaft, daß die transponierte Matrix gleich der konjugierten ist, d. h. daß

$$A' = \bar{A}, \tag{8}$$

heißt eine Hermitesche Matrix.

Durch Anwendung der Transformation (3) mit der Matrix B und der konjugierten Transformation

$$y_i = \sum_{k=1}^{n} \bar{b}_{ik} Y_k \qquad (i = 1, \ldots, n) \tag{9}$$

mit der konjugierten Matrix $\bar{B}$ geht (vgl. Kap. III, Satz 7) (6) in eine Form mit der Matrix $A_1 = B'A\bar{B}$ über. Aus (7) folgt dann, daß $A_1' = \bar{B}'A'B = \bar{A}$), d. h.:

Satz 3: Durch eine lineare Transformation mit der Matrix B und die konjugierte Transformation geht eine Hermitesche bilineare Form mit der Hermiteschen Matrix A wieder in eine Hermitesche bilineare Form, und zwar mit der Hermiteschen Matrix $B'A\bar{B}$, über.

Nennt man zwei $n$reihige quadratische Matrizen A und A_1 mit Elementen aus K in K verschwistert, wenn eine nicht singu-

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

läre $n$reihige quadratische Matrix B mit Elementen aus K existiert, so daß $A_1 = B'A\bar{B}$ ist, so erhält Satz 3 die Gestalt:

Satz 4: Zwei Hermitesche bilineare Formen mit Koeffizienten aus K sind dann und nur dann äquivalent gegenüber einer nichtsingulären Transformation und ihrer konjugierten mit Koeffizienten aus K, wenn ihre Matrizen in K verschwistert sind.

Setzen wir in (6) $y_k = \bar{x}_k$, so erhalten wir die Hermitesche Form

$$\sum_{i,k=1}^{n} a_{ik} x_i \bar{x}_k, \quad \text{in der} \quad a_{ik} = \bar{a}_{ki}. \tag{10}$$

Sie ist gleich ihrer konjugierten Form. Setzt man auch $Y_k = \bar{X}_k$, so gehen die entstehenden Gleichungen (9) aus (3) hervor, indem man überall die konjugierten Werte nimmt, d. h. (9) wird im wesentlichen mit (3) identisch. Satz 3 ergibt dann:

Satz 5: Durch eine lineare Transformation mit der Matrix B geht eine Hermitesche Form mit der Hermiteschen Matrix A über in eine Hermitesche Form mit der Hermiteschen Matrix $B'A\bar{B}$.

Oder, entsprechend Satz 4:

Satz 6: Zwei Hermitesche Formen mit Koeffizienten aus K sind dann und nur dann äquivalent gegenüber einer nichtsingulären Transformation mit Koeffizienten aus K, wenn ihre Matrizen in K verschwistert sind.

Durch Vergleichen von Satz 4 und 6 ergibt sich

Folgerung 2: Äquivalenten Hermiteschen bilinearen Formen entsprechen äquivalente Hermitesche Formen, und umgekehrt.

Auch hier wie in 33. sind also die beiden Äquivalenzprobleme nicht wesentlich voneinander verschieden, so daß unsere späteren Sätze über zwei quadratische bzw. Hermitesche Formen sich auch als Sätze über zwei symmetrische bzw. Hermitesche bilineare Formen aussprechen lassen.

Aber nicht nur, daß die beiden letzteren Probleme sich auf die beiden ersteren zurückführen lassen, sondern diese beiden ersteren können sogar, wie sogleich gezeigt werden soll, zusammen behandelt werden.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

35. Rationale Reduktion quadratischer und Hermitescher Formen. Wir stellen eine Abbildung des Körpers K auf sich selbst her, indem wir jedem Element a aus K ein Element $\tilde{a}$ aus K zuordnen, wobei diese Zuordnung die Eigenschaften haben soll, daß

$$\tilde{\tilde{a}} = a, \quad \widetilde{ag} = \tilde{a}\tilde{g}, \quad \widetilde{a \pm g} = \tilde{a} \pm \tilde{g}, \tag{11}$$

d. h. sie soll involutorisch[1]) und mit den ganzen rationalen Operationen vertauschbar sein. Einer Matrix $A = (a_{ik})$ mit Elementen aus K entspricht daher eine Matrix $\widetilde{A} = (\tilde{a}_{ik})$. Wie in (8) gilt also auch hier

$$\widetilde{\widetilde{A}} = A, \quad \widetilde{AQ} = \widetilde{A}\,\widetilde{Q}, \quad (\widetilde{A})' = \widetilde{A'}. \tag{12}$$ —

Läßt man wie in 34. K aus dem Unterkörper S durch Adjunktion von $\sqrt{v}$ hervorgehen, so sieht man, daß für das Zuordnungsgesetz $\tilde{a} = \bar{a}$ die Beziehungen (11) erfüllt sind. Desgleichen, wenn $\tilde{a} = a$ gesetzt wird. Wie wir sofort sehen werden, sind diese beiden Fälle die einzigen, die in der Theorie der Hermiteschen bzw. quadratischen Formen vorkommen.

Denn gehen wir aus von der Form

$$\sum_{i,k=1}^{n} a_{ik} x_i \tilde{x}_k, \quad \text{wo} \quad a_{ik} = \tilde{a}_{ki}, \tag{13}$$

mit Koeffizienten aus K, deren Matrix A also die Eigenschaft

$$A' = \widetilde{A} \tag{14}$$

besitzt, so geht unter der Annahme $\tilde{a} = \bar{a}$, $\tilde{x}_k = \overline{x}_k$ die Form (13) in die Hermitesche Form (10) über, deren Hermitesche Matrix also wirklich die Eigenschaft $A' = \overline{A}$ besitzt. Setzt man andererseits $\tilde{a} = a$, $\tilde{x}_k = x_k$, so erhält man aus (13) die quadratische Form (5), deren Matrix A symmetrisch ist und also die Eigenschaft $A' = A$ hat. Form (13) liefert also eine Verallgemeinerung der Hermiteschen und quadratischen Formen, die, wie man sehen wird, eine große Vereinfachung der Theorien dieser beiden Formenarten zur Folge hat.

---

1) Eine Transformation T heißt involutorisch, wenn sie nach zweimaliger Anwendung wieder auf die Ausgangsgröße zurückführt, so daß also $x\{T\}x_1\{T\}x$ für alle x gilt; kurz, in symbolischer Schreibweise, wenn $T^2 = 1$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 7: Jede Form (13) vom Range r mit Koeffizienten aus K kann durch eine nicht-singuläre Transformation[1]) mit Koeffizienten aus K auf die Gestalt gebracht werden

$$(15)\quad g_1 x_1 \tilde{x}_1 + \cdots + g_r x_r \tilde{x}_r, \text{ wo jedes } g_i \neq 0 \text{ und } \tilde{g}_i = g_i.$$

Wir dürfen in (13) $a_{11} \neq 0$ voraussetzen. Denn entweder erreicht man dies durch Umbenennen der x oder, wenn alle $a_{ii} = 0$ sind, hingegen etwa $a_{12} \neq 0$ ist, durch die Transformation

$$x_1 = X_1, \quad x_2 = gX_1 + X_2, \quad x_i = X_i \qquad (i>2);$$

denn dann geht (13) in $lX_1\widetilde{X}_1 + \cdots$ über, wo $l = a_{12}\tilde{g} + a_{21}g$, also z. B. gleich 2 wird, wenn man $g = \frac{1}{a_{21}}$ setzt.

Man kann also wegen $a_{11} \neq 0$ (13) auf die Gestalt bringen

$$\alpha = \frac{1}{a_{11}}\left(a_{11}x_1 + \sum_{i=2}^{n} a_{i1}x_i\right)\left(a_{11}\tilde{x}_1 + \sum_{k=2}^{n} a_{1k}\tilde{x}_k\right) + \varphi(x_2, \ldots, x_n, \tilde{x}_2, \ldots, \tilde{x}_n).$$

Bezeichnet man die Größe in der ersten Klammer mit $a_{11}X_1$, so wird in der zweiten gleich $a_{11}\widetilde{X}_1$, d. h. die Transformation

$$x_1 = X_1 - \frac{1}{a_{11}} \sum_{i=2}^{n} a_{i1}X_i, \quad x_k = X_k \qquad (k>1)$$

ersetzt α durch

$$a_{11}X_1\widetilde{X}_1 + \varphi(X_2, \ldots, X_n, \widetilde{X}_2, \ldots, \widetilde{X}_n).$$

Da nun die Matrizen von α und $a_{11}X_1\widetilde{X}_1$ die Eigenschaft (14) haben, so hat auch φ diese Eigenschaft. Wir können also mit φ ebenso verfahren wie mit (13) und erhalten schließlich die Form (15), deren Gliederzahl offenbar der Rang der Form und daher nach der letzten Fußnote auch der Rang von (13) ist.

Folgerung 3: In jedem Körper ist jede quadratische Form vom Rang r äquivalent mit

$$(16)\qquad g_1 x_1^2 + \cdots + g_r x_r^2, \text{ wo jedes } g_i \neq 0.$$

1) Nämlich durch die Transformation (3) zusammen mit der induzierten Transformation $\tilde{x}_i = \Sigma \tilde{b}_{ik}\widetilde{X}_k$. Die Matrix der resultierenden Form ist $B'A\widetilde{B}$ und hat denselben Rang wie A (nach Satz 6 in Kap. III).

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

36. Kanonische Formen. Ist K der Körper aller komplexen Zahlen, so läßt sich (16) durch die Transformation

$$x_i = g_i^{-\frac{1}{2}} \xi_i \qquad (i = 1, \ldots, r)$$

auf die Gestalt $\xi_1^2 + \cdots + \xi_r^2$ reduzieren.

Satz 8: Im Körper aller komplexer Zahlen kann durch eine nichtsinguläre lineare Transformation jede quadratische Form vom Range r auf die Gestalt $\xi_1^2 + \cdots + \xi_r^2$ gebracht werden. Zwei quadratische Formen sind hier also dann und nur dann äquivalent, wenn sie denselben Rang haben.

Hieraus und aus Folgerung 1 folgt

Folgerung 4: Zwei bilineare Formen sind im komplexen Zahlkörper dann und nur dann äquivalent, wenn sie denselben Rang r haben; sie lassen sich dann beide auf $\xi_1\eta_1 + \cdots + \xi_r\eta_r$ reduzieren.

Satz 9: K sei der Körper aller reellen bzw. aller komplexen Zahlen, je nachdem man $\tilde{a} = a$ bzw. $\overline{a} = \overline{a}$ für jedes a aus K setzt. Durch eine nicht singuläre Transformation mit Koeffizienten aus K läßt sich dann jede Form (13) vom Range r mit Koeffizienten aus K auf die Gestalt bringen

$$(17) \qquad y_1\overline{y}_1 + \cdots + y_p\overline{y}_p - y_{p+1}\overline{y}_{p+1} - \cdots - y_r\overline{y}_r,$$

wo der Index p eindeutig bestimmt ist. Daher sind zwei Formen (13) dann und nur dann in K äquivalent, wenn sie denselben Rang r und denselben Index p haben.

Da in (15) $\tilde{g}_i = g_i$, so ist jedes g_i reell. Durch Umbenennen der x in (15) können wir erreichen, daß $g_1, \ldots, g_p$ positiv und g_k $(k > p)$ negativ sind. Setzt man $g_k = -d_k$ $(k > p)$, so wird durch die reelle Transformation

$$x_i = g_i^{-\frac{1}{2}} y_i \qquad (i = 1, \ldots, p)$$

$$x_k = d_k^{-\frac{1}{2}} y_k \qquad (k = p+1, \ldots, r)$$

(15) in (17) übergeführt. Jede Form (13) vom Range r und mit Koeffizienten aus K läßt sich also durch eine nichtsinguläre Transformation[1]) mit Koeffizienten aus K auf die Gestalt (17) bringen.

Angenommen nun, es sei eine Darstellung

$$(18) \qquad z_1\tilde{z}_1 + \cdots + z_q\tilde{z}_q - z_{q+1}\tilde{z}_{q+1} - \cdots - z_r\tilde{z}_r$$

1) Die wohlgemerkt $x_1, \ldots, x_n$ durch $y_1, \ldots, y_n$ ausdrückt, nicht etwa nur durch $y_1, \ldots, y_r$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

möglich, bei der $q \neq p$, also etwa $p > q$ wäre. Dann sind also (17) und (18) nach Voraussetzung beide gleich der gegebenen Form (13), wenn die z und y als lineare Funktionen der $x_1, \ldots, x_n$ mit Koeffizienten aus K ausgedrückt werden, d. h. (17) und (18) sind identisch für alle x.

Nun hat das System der $q + n - p < n$ homogenen linearen Gleichungen

$$(19) \qquad z_1 = 0, \ldots, z_q = 0, \quad y_{p+1} = 0, \ldots, y_n = 0$$

in den n Unbekannten $x_1, \ldots, x_n$ die nichttrivialen Lösungen $x_1 = X_1, \ldots, x_n = X_n$ aus K (vgl. Kap. III, Satz 14, Folg.). Sind Y_i und Z_i die entsprechenden Werte von y_i und z_i, so erhält man durch Gleichsetzen von (17) und (18)

$$Y_1\widetilde{Y}_1 + \cdots + Y_p\widetilde{Y}_p = -Z_{q+1}\widetilde{Z}_{q+1} - \cdots - Z_r\widetilde{Z}_r.$$

Die Glieder links sind $\geqq 0$, während die rechts $\leqq 0$, infolgedessen sind alle Glieder $= 0$, insbesondere also $Y_1 = 0, \ldots, Y_r = 0$. Berücksichtigt man auch (19), so sieht man, daß das Gleichungssytem $y_1 = 0, \ldots, y_n = 0$ die nichttriviale Lösung $X_1, \ldots, X_n$ besitzt, daß also die Koeffizientendeterminante der x in $y_1, \ldots, y_n$ verschwindet. Mit anderen Worten, die Transformation, die (13) auf (17) reduziert, müßte singulär sein, gegen unsere Voraussetzung.

Trennt man die beiden Fälle von Satz 9, so erhält man

Folgerung 5: Jede reelle quadratische Form vom Range r läßt sich durch eine nichtsinguläre reelle Transformation auf die Gestalt bringen

$$(20) \qquad y_1^2 + \cdots + y_p^2 - y_{p+1}^2 - \cdots - y_r^2,$$

wo der Index p eindeutig bestimmt ist. Zwei reelle quadratische Formen sind also dann und nur dann gegenüber nichtsingulären reellen Transformationen äquivalent, wenn sie denselben Rang und denselben Index haben.[1])

Für $r = 2$ bekommen wir so die Typen $y_1^2 + y_2^2$, $y_1^2 - y_2^2$, $-y_1^2 - y_2^2$.

Eine quadratische $n$äre Form vom Range n liefert gleich Null gesetzt eine irreduzible quadratische Fläche im R_{n-1}, eine Form vom Range

1) Dieser Satz wurde von Jacobi (Journ. f. Math. 53, 1857, p. 275; Werke 4, 1884, p. 593) gefunden und unabhängig von ihm von Sylvester (Phil. Mag. (4), 4, 1852, p. 140; Phil. Trans., London 143, 1853, p. 481; Journ. f. Math. 100, 1887, p. 465; Coll. Math. Papers I, 1904, p. 376, p. 511; IV, p. 523. Letzterer nannte ihn das **Trägheitsgesetz der quadratischen Formen.**

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$r < n$ eine reduzible oder zerfallende Fläche. Satz 8 sagt nun aus, daß im komplexen Gebiet z. B. alle irreduziblen quadratischen Flächen linear ineinander transformierbar, d. h. also, daß sie äquivalent sind. Sie alle haben den Typus $x_1^2 + \cdots + x_n^2 = 0$.

Lasse ich aber nur reelle Transformationen zu, so habe ich nach Satz 9 je nach dem Index verschiedene Typen zu unterscheiden, z. B. bei den Kegelschnitten die Typen $x_1^2 + x_2^2 + x_3^2 = 0$, $x_1^2 + x_2^2 - x_3^2 = 0$; d. h. im Reellen besteht ein Unterschied zwischen Hyperbeln und Ellipsen.

Folgerung 6: Im Körper der komplexen Zahlen kann jede Hermitesche Form vom Range r auf die Gestalt

$$y_1\bar{y}_1 + \cdots + y_p\bar{y}_p - y_{p+1}\bar{y}_{p+1} - \cdots - y_r\bar{y}_r \tag{21}$$

gebracht werden, wo der Index p eindeutig bestimmt ist. Zwei Hermitesche Formen sind also dann und nur dann äquivalent, wenn sie denselben Rang r und denselben Index p haben.

Ebenso wie die Zahl r ohne Zurückgehen auf die kanonische Form bestimmt werden kann, so werden wir im Satz 22 auch zur Bestimmung von p eine direkte Methode kennenlernen. —

Aus Folgerung 1, 2, 5, 6 ergibt sich

Folgerung 7: Jede reelle bilineare symmetrische Form (bzw. jede Hermitesche bilineare Form mit komplexen Koeffizienten) kann durch nichtsinguläre reelle kogrediente Transformationen (bzw. durch eine nichtsinguläre Transformation der x und die konjugierte Transformation der y) auf eine einzige Weise auf die Gestalt gebracht werden

$$x_1y_1 + \cdots + x_py_p - x_{p+1}y_{p+1} - \cdots - x_ry_r. \; —$$

Eine reelle quadratische Form heißt positiv, wenn $r = p$, negativ, wenn $p = 0$. Erstere kann nur positive, letztere nur negative Werte annehmen. Beide heißen definitive Formen.

Positive und negative Hermitesche Formen werden ähnlich definiert.

37. Reduktion einer reellen quadratischen Form durch reelle orthogonale Transformationen. Wir haben im Vorhergehenden gesehen, welche Einflüsse eine Transformation auf eine der behandelten Formentypen hat, und wir haben die kanonischen Formen dieser Typen kennengelernt. Es ist nun — besonders für geometrische Anwendungen — oft von Wichtigkeit, nicht nur die kanonische Gestalt einer einzelnen Form zu kennen, sondern auch zu wissen, daß u. U. ein und dieselbe Transformation mehrere Formen gleichzeitig auf eine gemeinsame Gestalt bringen kann. Handelt es sich dabei um zwei Formen, so spricht man von

Digitized by Google Original from UNIVERSITY OF MICHIGAN

der „kanonischen Gestalt des Formenpaares". — Von gewissen Formenpaaren werden wir nun eine kanonische Gestalt angeben und dazu die folgenden beiden zusammengehörigen Sätze gleichzeitig beweisen:

Satz 10: Wenn f und h reelle n-äre quadratische Formen sind und wenn dabei h positiv und vom Range n ist, so kann das Paar f, h durch eine reelle nichtsinguläre lineare Transformation auf die Gestalt

$$f = \lambda_1 \xi_1^2 + \cdots + \lambda_n \xi_n^2, \quad h = \xi_1^2 + \cdots + \xi_n^2$$

gebracht werden, wo $\lambda_1, \ldots, \lambda_n$ sämtlich reell und die Wurzeln von $|f - \lambda h| = 0$ sind.

Satz 11: Wenn f und h zwei n-äre Hermitesche Formen sind und wenn dabei h positiv und vom Range n ist, so kann das Paar f, h durch eine nichtsinguläre lineare Transformation auf die Gestalt

$$f = \lambda_1 \xi_1 \bar{\xi}_1 + \cdots + \lambda_n \xi_n \bar{\xi}_n, \quad h = \xi_1 \bar{\xi}_1 + \cdots + \xi_n \bar{\xi}_n$$

gebracht werden, wo $\lambda_1, \ldots, \lambda_n$ sämtlich reell und die Wurzeln von $|f - \lambda h| = 0$ sind.

$A = (a_{ik})$ und $B = (b_{ik})$ seien die Matrizen von f und h. Dann hat das System der n linearen Gleichungen

$$\sum_{k=1}^{n} a_{ik} \tilde{x}_k = \lambda_1 \sum_{k=1}^{n} b_{ik} \tilde{x}_k \qquad (i = 1, \ldots, n)$$

in den n Unbekannten $\tilde{x}_k$ eine nichttriviale Lösung, wenn λ_1 eine Wurzel von $|A - \lambda_1 B| = 0$ ist. Infolgedessen ist für diese auch

$$f = \sum_{i,k} a_{ik} x_i \tilde{x}_k = \sum_i x_i \cdot \lambda_1 \sum_k b_{ik} \tilde{x}_k = \lambda_1 h, \quad \text{wo} \quad h = \sum_{i,k} b_{ik} x_i \tilde{x}_k.$$

f und h seien nun zunächst Hermitesche Formen. Dann ist h, da es nach Voraussetzung positiv und vom Range n ist, für jene in Frage kommenden Lösungswerte der $\tilde{x}_k$ von Null verschieden. Und da f und h reell sind, so ist auch λ_1 reell, d. h. alle Wurzeln von $|A - \lambda B| = 0$ sind reell.

Nunmehr sei h eine reelle positive quadratische Form. Aus den Koeffizienten von h baue man sich eine Hermitesche Form $H = \Sigma b_{st} x_s \bar{x}_t$, wo $\bar{x}_t$ der konjugiert komplexe Wert von x_t ist. Setzt man dann $x_s = \xi_s + i\eta_s$, so ist H die Summe der Ausdrücke $\Sigma b_{st} \xi_s \xi_t$ und $\Sigma b_{st} \eta_s \eta_t$, die beide $\geqq 0$ sind. D. h. es ist auch $H \geqq 0$, und zwar > 0, wenn nicht alle x gleich Null sind. Für die Hermitesche Form $F = \Sigma a_{st} x_s \bar{x}_t$ und die positive Form H ist also die Wurzel λ_1 von $|A - \lambda B| = 0$ nach dem vorher-

Digitized by Google Original from UNIVERSITY OF MICHIGAN

gehenden Fall reell. Die Formen f und h haben aber dieselben Matrizen A bzw. B, so daß auch für sie λ_1 reell ist. —

Es ist also $f - \lambda_1 h$ eine reelle quadratische bzw. Hermitesche Form. Da ihre Determinante verschwindet, so läßt sie sich nach Satz 7 durch eine nichtsinguläre Transformation, die im Falle der quadratischen Form reell ist, auf eine reelle quadratische bzw. Hermitesche Form $F(y_2, \ldots, y_n)$ von $n-1$ Variabeln reduzieren. Durch dieselbe Transformation möge h in H übergehen, so daß

$$f - \lambda h \equiv f - \lambda_1 h + (\lambda_1 - \lambda) h \quad \text{in}$$

$$f - \lambda h \equiv F(y_2, \ldots, y_n) + (\lambda_1 - \lambda) H(y_1, \ldots, y_n) \tag{22}$$

übergeht.

Da nun in der positiven Form H vom Range n der Koeffizient von $y_1 \tilde{y}_1$ nicht verschwindet, da sonst für das Wertsystem $y_1 = 1$, $y_k = 0$ $(k > 1)$ auch H verschwinden würde, so existiert nach dem letzten Teil des Beweises von Satz 7 eine nichtsinguläre lineare Transformation, die jedes $y_k (k > 1)$ ungeändert läßt, hingegen H durch eine Form $c_1 g_1 \tilde{g}_1 + \psi(y_2, \ldots, y_n)$ ersetzt, wo $c_1 \neq 0$, also bei uns $c_1 > 0$ ist. Diese Transformation, die im Falle quadratischer Formen reell ist, ersetzt die rechte Seite von (22) durch

$$F(y_2, \ldots, y_n) + (\lambda_1 - \lambda) c_1 g_1 \tilde{g}_1 + (\lambda_1 - \lambda) \psi(y_2, \ldots, y_n).$$

Setzt man für $F + \lambda_1 \psi$ einfach φ, so ist also

$$f - \lambda h \equiv \varphi(y_2, \ldots, y_n) + (\lambda_1 - \lambda) c_1 g_1 \tilde{g}_1 - \lambda \cdot \psi(y_2, \ldots, y_n).$$

Hieraus erhält man durch Gleichsetzen entsprechender Potenzen von λ

$$f \equiv \lambda_1 c_1 g_1 \tilde{g}_1 + \varphi(y_2, \ldots, y_n), \quad h \equiv c_1 g_1 \tilde{g}_1 + \psi(y_2, \ldots, y_n).$$

Gemäß der über h gemachten Annahme ist ψ offenbar > 0 und vom Rang $n-1$. Sind nun f und h zwei quadratische Formen, die durch eine nichtsinguläre lineare Transformation B in F und H übergehen, so ist (nach 33.) $F = B' f B$ und $H = B' h B$, also $|F - \lambda H| = |B|^2 \cdot |f - \lambda h|$, d. h. $|F - \lambda H| = 0$ hat dieselben Wurzeln wie $|f - \lambda h| = 0$. Dasselbe gilt für Hermitesche Formen, denn dort ist $|F - \lambda H| = |B| \cdot |\bar{B}| \cdot |f - \lambda h|$. — Auf unseren Fall angewandt, heißt dies, daß $(\lambda_1 - \lambda)|\varphi - \lambda \psi| = 0$ dieselben Wurzeln hat wie $|f - \lambda h| = 0$. Ist demnach λ_2 eine andere Wurzel von $|f - \lambda h| = 0$, so ist unsere obige Reduktion auch auf φ, ψ und λ_2 anwendbar und führt zu einer Abspaltung der Glieder $\lambda_2 c_2 g_2 \tilde{g}_2$ und $c_2 g_2 \tilde{g}_2$. — So sieht man, daß durch eine

Digitized by Google Original from UNIVERSITY OF MICHIGAN

nichtsinguläre Transformation, die zudem im Falle quadratischer Formen reell ist, f und h auf die Gestalt

$$f \equiv \sum \lambda_i c_i g_i \bar{g}_i, \quad h \equiv \sum c_i g_i \bar{g}_i$$

gebracht werden können, wo alle $c_i > 0$ sind. Schließlich erhält man durch die reelle nichtsinguläre Transformation

$$\xi_i = \sqrt{c_i}\, g_i \qquad (i = 1, \ldots, n)$$

die gewünschte endgültige Form.

Zugleich sieht man, daß alle Formen des Büschels $f + \mu h$, wo der Parameter μ alle reellen Werte von $+\infty$ bis $-\infty$ durchlaufen kann, vermittels derselben Basis $\xi_1, \ldots, \xi_n$ darstellbar sind.

Einen speziellen Fall von Satz 10 erhält man, wenn man $h = x_1^2 + \cdots + x_n^2$ setzt. Dann führt unsere lineare Transformation h wieder in eine Quadratsumme, nämlich $\xi_1^2 + \cdots + \xi_n^2$, über, läßt also h ungeändert. Sie heißt in diesem Falle orthogonal.[1]) Ähnlich heißt die Transformation, die $h = x_1 \bar{x}_1 + \cdots + x_n \bar{x}_n$ ungeändert läßt, unitär. Die Sätze 10 und 11 gehen dann in die beiden folgenden über:

Satz 12: Wenn f eine reelle quadratische Form mit der Matrix A ist, so sind die Wurzeln $\lambda_1, \ldots, \lambda_n$ ihrer charakteristischen Gleichung $|A - \lambda E| = 0$ sämtlich reell, und f kann durch eine reelle orthogonale Transformation auf die Gestalt $\Sigma \lambda_i \xi_i^2$ gebracht werden.

Satz 13: Wenn f eine Hermitesche Form mit der Matrix A ist, so sind die Wurzeln $\lambda_1, \ldots, \lambda_n$ ihrer charakteristischen Gleichung $|A - \lambda E| = 0$ sämtlich reell, und f kann durch eine unitäre Transformation auf die Gestalt $\Sigma \lambda_i \xi_i \bar{\xi}_1$ gebracht werden.

Übungen: 1. Eine lineare Transformation mit der Matrix B ist dann und nur dann orthogonal bzw. unitär, wenn $B'B = E$ bzw. $B'\bar{B} = E$ ist. — Denn man hat ja in 33. bzw. 34. nur $A = A_1 = E$ zu setzen.

2. Die Determinante einer orthogonalen bzw. unitären Transformation ist gleich ± 1 bzw. vom absoluten Betrage 1.

3. Das Produkt zweier orthogonalen Transformationen und die Inverse einer orthogonalen Transformation sind wieder orthogonal. Ebenso für unitäre Transformationen.

4. Wenn eine lineare Transformation zwei der folgenden Eigenschaften besitzt: 1. sie ist reell, 2. sie ist orthogonal, 3. sie ist unitär, so besitzt sie auch die dritte Eigenschaft.

---

1) Betr. des Namens „orthogonal" sehe man Übung 7.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

5. Jede reelle orthogonale Transformation von x und y ist von der Form

$$x' = x \cdot \cos\alpha - y \cdot \sin\alpha, \quad y' = \pm (x \cdot \sin\alpha + y \cdot \cos\alpha).$$

6. Die Matrix jeder unitären unimodularen Transformation zweier Variabeln ist von der Form $\begin{pmatrix} a & -\bar{c} \\ c & \bar{a} \end{pmatrix}$.

7. Der Name „orthogonal" stammt daher, daß, wenn ich ein rechtwinkliges Koordinatensystem um den Ursprung drehe, ich die neuen Koordinaten aus den alten durch eine orthogonale Transformation erhalte. Denn da diese Drehung die „Kugel" $x_1^2 + \cdots + x_n^2 = r^2$ im Raume R_n (von der $n$ten Dimension) in sich selbst überführt, so muß auch $\xi_1^2 + \cdots + \xi_n^2 = r^2$, also $x_1^2 + \cdots + x_n^2 = \xi_1^2 + \cdots + \xi_n^2$ sein, da zwei Funktionen, die für ein Kontinuum von Punkten miteinander übereinstimmen, überhaupt identisch sind. — Man zeige, daß nach Satz 12 die Gleichung jeder reellen quadratischen Fläche im R_3 sich auf eine Form reduzieren läßt, in der die Glieder zweiten Grades gleich $a x_1^2 + b x_2^2 \pm c x_3^2$ oder $a x_1^2 \pm b x_2^2$ oder $a x_1^2$ sind, wo $a > 0$, $b > 0$, $c > 0$.

8. In der kanonischen Form (20) ist die Zahl der positiven Glieder gleich p, die der negativen gleich $N = r - p$. Man führt nun oft die neue Größe $p - N$ ein und nennt sie die Signatur. Dann sind zwei reelle quadratische Formen dann und nur dann äquivalent gegenüber reellen Transformationen, wenn sie denselben Rang und dieselbe Signatur haben.

9. Satz 10 liefert für $n = 3$ (bzw. 4) den geometrischen Satz: Zwei Kurven (bzw. Flächen) zweiter Ordnung, von denen mindestens eine irreduzibel ist, haben stets ein gemeinsames reelles Polardreieck (bzw. -tetraeder).

38. Der Rang einer symmetrischen und einer Hermiteschen Matrix.

Satz 14: Wenn eine r-reihige Determinante d einer Matrix nicht verschwindet, hingegen wohl alle $(r+1)$reihigen Determinanten, welche d als ersten Minor haben, gleich Null sind, so ist die Matrix vom Range r.

Man beachte, daß dieser Satz das Aufsuchen der Rangzahl r bedeutend abkürzt, da wir nach ihm nicht mehr alle $(r+1)$-reihigen Determinanten zu untersuchen brauchen, sondern nur diejenigen, die d als ersten Minor haben.

Die Matrix A und die Determinante d können in der Form

$$A = \begin{pmatrix} a_{11} \cdots a_{1n} \\ \cdots \\ a_{m1} \cdots a_{mn} \end{pmatrix}, \quad d = \begin{vmatrix} a_{11} \cdots a_{1r} \\ \cdots \\ a_{r1} \cdots a_{rr} \end{vmatrix} \neq 0$$

vorausgesetzt werden. Jetzt führe man die Größen ein

$$l_i = a_{i1} y_1 + \cdots + a_{in} y_n,$$
$$\lambda_i = a_{i1} y_1 + \cdots + a_{ir} y_r, \qquad (i = 1, \ldots, m)$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Unser Satz ist bewiesen, wenn wir gezeigt haben, daß mehr als r der Formen l_i voneinander linear abhängig sind. Für $s > r$, $t > r$ ist nun die $(r+1)$reihige Determinante der Formen

$$\lambda_i + a_{it} y_t \qquad (i = 1, \ldots, r, s),$$

da sie d als ersten Minor besitzt, gleich Null. Also sind diese $r+1$ Formen nach Kap. III, Satz 9 linear abhängig, so daß

$$\lambda_s + a_{st} y_t = \sum_{i=1}^{r} c_i (\lambda_i + a_{it} y_t). \tag{23}$$

Wegen $d \neq 0$ können wir die Gleichungen $\lambda_i = a_{i1} y_1 + \cdots + a_{ir} y_r$ $(i = 1, \ldots, r)$ auflösen und $y_1, \ldots, y_r$ linear durch $\lambda_1, \ldots, \lambda_r$ ausdrücken. Durch Substitution in λ_s erhält man

$$\lambda_s = b_1 \lambda_1 + \cdots + b_r \lambda_r.$$

Setzt man dies in (23) ein und berücksichtigt, daß $y_1, \ldots, y_r, y_t$, also auch $\lambda_1, \ldots, \lambda_r, y_t$ linear unabhängig sind, so sieht man, daß

$$c_i = b_i \quad (i = 1, \ldots, r), \qquad a_{st} = \sum_{i=1}^{r} b_i a_{it}.$$

Jetzt ist

$$l_s \equiv \lambda_s + \sum_{t=r+1}^{n} a_{st} y_t = \sum_{i=1}^{r} b_i (\lambda_i + \sum_{t=r+1}^{n} a_{it} y_t) \equiv \sum_{i=1}^{r} b_i l_i.$$

Damit ist unser Ziel erreicht: $l_{r+1}, \ldots, l_m$ sind lineare Funktionen von $l_1, \ldots, l_r$, d. h. mehr als r der Formen l_i sind linear abhängig.

Wir wollen nunmehr Sätze beweisen, mittels deren wir den Rang einer Matrix A mit der Eigenschaft $A' = \widetilde{A}$ durch alleinige Untersuchung der Hauptminoren finden können. Ein Hauptminor einer Determinante A ist ein solcher, der aus A durch Tilgung gleichstelliger Reihen und Spalten hervorgeht, dessen Diagonalelemente also unter den Diagonalelementen von A vorkommen.

Satz 15: Es liege eine symmetrische oder eine Hermitesche Matrix A vor. Einer ihrer r-reihigen Hauptminoren p_r sei $\neq 0$, hingegen seien alle Hauptminoren, die man aus p_r durch Hinzufügung einer sowie zweier Reihen und Spalten von A erhält, gleich Null. Dann ist der Rang von A gleich r.

Wieder dürfen wir annehmen, daß p_r aus den Elementen der r ersten Zeilen und Spalten von $A = (a_{ij})$ besteht. — Wir brauchen nun nicht von allen $(r+1)$reihigen Determinanten von A

Digitized by Google Original from UNIVERSITY OF MICHIGAN

zu beweisen, daß sie verschwinden, sondern nach Satz 14 genügt es zu zeigen, daß alle $g_{ij} = 0$ sind, wobei g_{ij} eine Determinante ist, die aus p_r durch Hinzufügung einer beliebigen $i$ten Zeile und $j$ten Spalte von A hervorgeht. Bezeichnet man nun die Determinante, die man aus p_r durch Hinzufügung der $i$ten und $j$ten Zeile und Spalte von A erhält, mit c und die zu a_{ij} in c gehörige Unterdeterminante mit A_{ij}, so ist nach einem Hauptsatz über Determinanten

$$c \cdot p_r = \begin{vmatrix} A_{ii} & A_{ij} \\ A_{ji} & A_{jj} \end{vmatrix} = g_{jj}g_{ii} - g_{ij}g_{ji}. \tag{24}$$

Nun ist nach Voraussetzung $g_{ii} = 0$, $g_{jj} = 0$, $c = 0$. Da ferner $A' = \widetilde{A}$ ist und man aus g_{ji} durch Vertauschung der Zeilen und Spalten die Determinante $\tilde{g}_{ij}$ bekommt, so ist $g_{ji} = \tilde{g}_{ij}$, also

$$0 = g_{ij}g_{ji} = g_{ij}\tilde{g}_{ij}, \quad \text{d. h.} \quad g_{ij} = 0.$$

Satz 16: Wenn alle $(r+1)$reihigen und alle $(r+2)$reihigen Hauptminoren einer symmetrischen oder einer Hermiteschen Matrix A verschwinden, so ist der Rang von A höchstens gleich r.

Der Satz ist offenbar richtig, wenn $r = 0$ ist, da aus $a_{ii} = a_{jj} = 0$ und $a_{ii}a_{jj} - a_{ij}a_{ji} = 0$ folgt, daß $a_{ij}\tilde{a}_{ij} = 0$, d. h. daß alle a_{ij} verschwinden. Infolgedessen besitzt A den Rang Null.

Wir werden den Satz also für $r = k$ als richtig voraussetzen und beweisen, daß er dann auch für $r = k + 1$ richtig ist. In letzterem Fall sind nach Voraussetzung alle $(k+2)$reihigen und alle $(k+3)$reihigen Hauptminoren gleich Null. Sind außerdem noch alle $(k+1)$reihigen Hauptminoren gleich Null, so ist, da der Satz für $r = k$ gilt, der Rang von A höchstens gleich k. Verschwinden indessen nicht alle $(k+1)$reihigen Hauptminoren, so ist nach Satz 15 der Rang gleich $k+1$. In beiden Fällen ist also der Rang $\leqq k+1$, womit unser Induktionsschluß bewiesen ist.

Satz 17: Jede symmetrische oder Hermitesche Matrix vom Range $r (r > 0)$ enthält mindestens einen von Null verschiedenen r-reihigen Hauptminor.

Alle $(r+1)$reihigen Hauptminoren verschwinden; wären auch alle $r$reihigen Hauptminoren gleich Null, so wäre nach Satz 16 der Rang $\leqq r - 1$.

Übungen: 1. Beweise mit Satz 16, daß der Rang folgender Matrix gleich 2 ist:

$$\begin{pmatrix} -6 & -5 & 1 & -2 \\ -5 & 56 & 4 & 11 \\ 1 & 4 & 0 & 1 \\ -2 & 11 & 1 & 2 \end{pmatrix}.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

2. Eine Matrix A heißt schiefsymmetrisch, wenn $A' = -A$. Alle ihre Hauptminoren ungerader Ordnung verschwinden. Man dehne die Sätze 15 bis 17 auf schiefsymmetrische Matrizen aus. Mit Satz 17 beweise man dann, daß der Rang einer solchen Matrix immer grade ist.

3. Wenn A eine reelle schiefsymmetrische Matrix ist, so ist $P = iA$ eine Hermitesche Matrix. Hieraus leite man einen direkten Beweis von Übung 2 ab. Die charakteristische Gleichung $|A - \lambda E| = 0$ einer reellen schiefsymmetrischen Matrix hat nur rein imaginäre Wurzeln.

4. Eine bilineare Form heißt alternierend, wenn $a_{ik} = -a_{ki}$, ihre Matrix also schiefsymmetrisch ist. Ist $a_{12} \neq 0$, so zeige man, daß durch die Transformation

$$x_2 = a_{12}^{-1}\Big(X_2 - \sum_{k=3}^{n} a_{1k} X_k\Big), \quad x_i = X_i \qquad (i = 1, 3, 4, \ldots, n)$$

und durch die kogrediente Transformation der y die bilineare Form a in $X_1 Y_2 - X_2 Y_1 + \varphi$ übergeht, wo φ eine alternierende bilineare Form in X_i, Y_i $(i = 2, \ldots, n)$ allein ist. Behandelt man φ ebenso wie a, so folgt leicht, daß jede alternierende bilineare Form a mit Koeffizienten in irgendeinem Körper K durch nicht singuläre kogrediente Transformationen mit Koeffizienten aus K auf die Gestalt

$$\xi_1 \eta_2 - \xi_2 \eta_1 + \xi_3 \eta_4 - \xi_4 \eta_3 + \cdots + \xi_{2s-1} \eta_{2s} - \xi_{2s} \eta_{2s-1}$$

gebracht werden kann.

5. Unter einer alternierenden Hermiteschen bilinearen Form a versteht man eine solche, für die $a_{ik} = -\bar{a}_{ki}$, $B = iA$ ist eine Hermitesche Matrix. Welches ist daher die kanonische Form von a?

Satz 18: Wenn M eine symmetrische oder Hermitesche Matrix vom Range $r > 0$ ist, so können wir aus M durch Vertauschung der Zeilen und die gleichartige Vertauschung der Spalten eine reguläre symmetrische bzw. Hermitesche Matrix $A = (a_{ij})$ erhalten, d. h. eine Matrix von der Beschaffenheit, daß von den Hauptminoren

$$(25) \quad p_0 = 1, \quad p_1 = a_{11}, \quad p_2 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \ldots, p_r = \begin{vmatrix} a_{11} \ldots a_{1r} \\ \cdots\cdots\cdots \\ a_{r1} \ldots a_{rr} \end{vmatrix}$$

keine zwei aufeinander folgenden verschwinden und daß der letzte Minor $p_r \neq 0$ ist.

Wir sehen zunächst von dem Fall, wo alle Diagonalelemente von M verschwinden, ab. Es sei daher das $i$te Element von Null verschieden. Durch gleichartiges Umnumerieren von Zeilen und Spalten erhält man aus M eine Matrix M_1 mit $a_{11} \neq 0$.

Sehen wir wiederum von dem Fall ab, wo alle zweireihigen Hauptminoren von M_1, die a_{11} enthalten, verschwinden. Dann

Digitized by Google Original from UNIVERSITY OF MICHIGAN

können wir auch hier durch Umnumerieren einen der nicht verschwindenden Minoren an erste Stelle bringen und so aus M_1 eine Matrix M_2 erhalten, bei der $a_{11} \neq 0$ und $a_{11}a_{22} - a_{12}a_{21} \neq 0$.

Dieses Verfahren läßt sich weiter fortsetzen, und es bleibt schließlich eine Matrix M_r übrig, bei der keine der Zahlen (25) verschwindet, vorausgesetzt, daß nicht einer der erwähnten Fälle eintritt. Es seien also die Zahlen $p_1 = a_{11}, p_2, \ldots, p_k$ von Null verschieden, jedoch seien alle $(k+1)$reihigen Hauptminoren, die p_k als ersten Minor enthalten, gleich Null ($k < r$). Nach Satz 15 ist aber dann nicht jeder $(k+2)$reihige Hauptminor, der p_k als zweiten Minor enthält, gleich Null, weil sonst der Rang von M gleich k, also $< r$ wäre. Durch Umnumerieren kann man wieder erreichen, daß $p_{k+1} = 0$, $p_{k+2} \neq 0$.

Um den Satz jetzt induktiv zu beweisen, nehme man an, man habe eine Matrix B erhalten, in der keine zwei aufeinanderfolgenden der Zahlen $p_1, \ldots, p_s$ verschwinden, wo $p_s \neq 0$, $s < r$. Wenn jetzt nicht alle $(s+1)$reihigen Hauptminoren von B, welche p_s als ersten Minor besitzen, verschwinden, so können wir wieder die Zeilen und Spalten von der Ordnung $s+1, \ldots, n$ vertauschen und erhalten eine Matrix, in der auch $p_{s+1} \neq 0$. Im Gegenfall verfahren wir wie im vorigen Absatz, wo jetzt $k = s$, und erhalten eine Matrix mit $p_{s+2} \neq 0$, $p_{s+1} = 0$.

39. Die Kroneckersche Reduktionsmethode.[1])

Satz 19: Es sei

$$Q = \tilde{Q} = \sum_{i,j=1}^{n} a_{ij} x_i \tilde{x}_j, \quad a_{ji} = \tilde{a}_{ij} \tag{26}$$

eine quadratische oder Hermitesche Form vom Range r ($0 < r < n$) mit Koeffizienten aus K. Es sei $|a_{ij}| \neq 0$ $(i,j = 1, \ldots, r)$. Dann können wir durch eine unimodulare lineare Transformation mit Koeffizienten aus K an Stelle der x neue Variabeln y einführen, so daß $x_i = y_i$ für $i = r+1, \ldots, n$ wird und daß Q in

$$Q_1 = \sum_{i,j=1}^{r} a_{ij} y_i \tilde{y}_j$$

übergeht, dessen Glieder dieselben Koeffizienten haben wie die entsprechenden Glieder von Q.

---

1) Werke I, p. 166, p. 357. Vgl. auch Dickson, Trans. Amer. Math. Soc. 10, 1909, p. 129.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Zunächst ist die Forderung, daß $|a_{ij}| \neq 0$, keine Beschränkung, denn durch Umnumerieren können wir dies leicht erreichen (s. Satz 17). — Je nachdem nun $\tilde{x}$ für x oder $\bar{x}$ steht, sei $t = 2$ oder 1. Dann ist

$$\frac{\partial Q}{\partial x_i} = t \sum_{j=1}^{n} a_{ij} \tilde{x}_j \qquad (i = 1, \ldots, n).$$

Da die Determinante dieser n linearen Formen vom Range r ist, so sind nach Satz 10 und 13 von Kap. III r unter ihnen (und zwar die r ersten) linear unabhängig, während die $n - r$ übrigen linear von ihnen abhängen:

$$\frac{\partial Q}{\partial x_k} = \sum_{i=1}^{r} c_{ki} \frac{\partial Q}{\partial x_i} \qquad (k = r+1, \ldots, n), \tag{27}$$

wo die c_{ki} Zahlen aus K sind. Man übe nun die unimodulare Transformation

$$x_i = y_i - \sum_{k=r+1}^{n} c_{ki} y_k \qquad (i = 1, \ldots, r), \tag{28}$$

$$x_k = y_k \qquad (k = r+1, \ldots, n)$$

mit der dazugehörigen

$$\tilde{x}_i = \tilde{y}_i - \sum_{k=r+1}^{n} \tilde{c}_{ki} \tilde{y}_k \qquad (i = 1, \ldots, r), \tag{29}$$

$$\tilde{x}_k = \tilde{y}_k \qquad (k = r+1, \ldots, n)$$

aus. Dann ist

$$\frac{\partial Q}{\partial y_k} = \sum_{i=1}^{n} \frac{\partial Q}{\partial x_i} \cdot \frac{\partial x_i}{\partial y_k} = \frac{\partial Q}{\partial x_k} - \sum_{i=1}^{r} c_{ki} \frac{\partial Q}{\partial x_i} = 0 \qquad (k = r+1, \ldots, n)$$

und, da $Q = \tilde{Q}$,

$$\frac{\partial Q}{\partial \tilde{y}_k} = \frac{\partial \tilde{Q}}{\partial \tilde{y}_k} = \sum_{i=1}^{n} \frac{\partial \tilde{Q}}{\partial \tilde{x}_i} \cdot \frac{\partial \tilde{x}_i}{\partial \tilde{y}_k} = \frac{\partial \tilde{Q}}{\partial \tilde{x}_k} - \sum_{i=1}^{r} \tilde{c}_{ki} \frac{\partial \tilde{Q}}{\partial \tilde{x}_i} = 0 \qquad (k = r+1, \ldots, n),$$

wie sich aus (27) ergibt. Wir haben damit Q in eine Form Q_1 transformiert, in der y_k und $\tilde{y}_k$ $(k = r+1, \ldots, n)$ überhaupt nicht vorkommen. Man erhält also Q_1 aus Q, indem man $x_i = y_i$, $\tilde{x}_i = \tilde{y}_i$ $(i = 1, \ldots, r)$ und $x_k = \tilde{x}_k = 0$ $(k = r+1, \ldots, n)$ setzt. In Q_1 haben wir die gesuchte Form gefunden.

In den folgenden beiden Sätzen bedeutet A_{ij} wie gewöhnlich die Unterdeterminante von a_{ij}.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 20: Wenn $A_{nn} \neq 0$, so können wir durch eine unimodulare lineare Transformation (mit Koeffizienten aus K) an Stelle der x neue Variabeln y einführen, so daß $x_n = y_n$ wird und daß (26) *in*

$$\sum_{i,j=1}^{n-1} a_{ij} y_i \tilde{y}_j + \frac{a}{A_{nn}} y_n \tilde{y}_n \quad \textit{übergeht.} \tag{30}$$

Zum Beweis betrachte man die Form

$$\varphi = \sum_{i,j=1}^{n} a_{ij} x_i \tilde{x}_j - \frac{a}{A_{nn}} \cdot x_n \tilde{x}_n .$$

Ihre Determinante erhält man aus a, indem man a_{nn} durch $a_{nn} - \frac{a}{A_{nn}}$ ersetzt; sie ist daher gleich der Summe von a und einer Determinante, die man aus a erhält, wenn man die letzte Zeile durch $0, \ldots, 0, -\frac{a}{A_{nn}}$ ersetzt. Daher ist die Determinante von φ gleich

$$a - A_{nn} \cdot \frac{a}{A_{nn}} = 0 ,$$

also hat φ den Rang $n-1$. Nach Satz 19 existiert daher eine Transformation von der in unserem Satz angegebenen Form, welche φ in

$$\sum_{i,j=1}^{n-1} a_{ij} y_i \tilde{y}_j$$

und $x_n \tilde{x}_n$ in $y_n \tilde{y}_n$ und daher auch (26) in (30) überführt.

Satz 21: Wenn $A_{nn} = 0$, $A_{n-1,n-1} = 0$, $A_{n,n-1} \neq 0$, so können wir durch eine unimodulare lineare Transformation mit Koeffizienten aus K an Stelle der x neue Variabeln y einführen, so daß $x_{n-1} = y_{n-1}$, $x_n = y_n$ wird und daß (26) *übergeht in*

$$\sum_{i,j=1}^{n-2} a_{ij} y_i \tilde{y}_j + g y_{n-1} \tilde{y}_n + \tilde{g} y_n \tilde{y}_{n-1}, \quad \textit{wo} \quad g = \frac{a}{\tilde{A}_{n,n-1}} . \tag{31}$$

Mit b bezeichne man die Determinante, die aus a durch Tilgung der beiden letzten Zeilen und Spalten entsteht. Dann ist wie in (24)

$$ab = \begin{vmatrix} A_{n-1,n-1} & A_{n-1,n} \\ A_{n,n-1} & A_{n,n} \end{vmatrix} = -A_{n,n-1} \tilde{A}_{n,n-1} \neq 0 . \tag{32}$$

Jetzt betrachte man die Form

$$\varphi = \sum_{i,j=1}^{n} a_{ij} x_i \tilde{x}_j - g x_{n-1} \tilde{x}_n - \tilde{g} x_n \tilde{x}_{n-1} .$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ihre Matrix ist

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1,n-1} & a_{1,n} \\ \cdot & \cdots & \cdot & \cdot \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} - g \\ a_{n,1} & \cdots & a_{n,n-1} - \tilde{g} & a_{n,n} \end{pmatrix}.$$

Auch hier ist die Determinante, die man durch Tilgung der beiden letzten Zeilen und Spalten erhält, gleich b. Wegen (32) verschwindet sie nicht und ist die Größe p_r von Satz 15. Ferner ist der Hauptminor von M, der durch Tilgung der letzten Zeile und Spalte entsteht, gleich $A_{nn} = 0$ und derjenige, der durch Tilgung der vorletzten Zeile und Spalte entsteht, gleich $A_{n-1,n-1} = 0$. [Dies sind die einzigen $(n-1)$ reihigen Hauptminoren, die b als ersten Minor besitzen.] Bezeichnet endlich d die Determinante von M, so zeigt derselbe Satz, aus dem sich eben (32) ergab, daß

$$db = \begin{vmatrix} A_{n-1,n-1} & A_{n-1,n} + \tilde{g} b \\ A_{n,n-1} + g b & A_{n,n} \end{vmatrix} = -t\tilde{t},$$

wo $t = A_{n,n-1} + gb$. Denn es ist $b = \tilde{b}$ und $A_{n,n-1} = \tilde{A}_{n-1,n}$. Ersetzt man nunmehr g durch seinen Wert aus (31), so erhält man mit Benutzung von (32)

$$\tilde{A}_{n,n-1} t = b(g\tilde{A}_{n,n-1} - a) = 0,$$

also $t = 0$, $db = 0$ und schließlich $d = 0$. Demnach besitzt M nach Satz 15 den Rang $n-2$, und nach Satz 19 existiert eine Transformation von der in Satz 21 angegebenen Art, welche φ durch

$$\sum_{i,j=1}^{n-2} a_{ij} y_i \tilde{y}_j$$

und also (26) durch (31) ersetzt. —

Wenden wir auf (31) noch die Transformation

$$y_i = x_i, \quad y_{n-1} = x_{n-1} - \frac{1}{2}\tilde{g} x_n, \qquad (i = 1, \ldots n-2)$$

$$y_n = \left(\frac{1}{\tilde{g}}\right) x_{n-1} + \frac{1}{2} x_n$$

von der Determinante 1 an, so erhalten wir

$$(33) \quad \sum_{i,j=1}^{n-2} a_{ij} x_i \tilde{x}_j + 2 x_{n-1}\tilde{x}_{n-1} - \frac{1}{2} g\tilde{g} x_n \tilde{x}_n, \quad g = \frac{a}{\tilde{A}_{n,n-1}}.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Vermittels der Sätze 19—21 können wir nun eine lineare unimodulare Transformation mit Koeffizienten aus K finden, durch die eine Form Q mit Koeffizienten aus K vom Range r in

$$g_1 x_1 \tilde{x}_1 + \cdots + g_r x_r \tilde{x}_r \qquad (g_i = \tilde{g}_i \neq 0), \tag{34}$$

übergeht. Die g erhält man aus den Koeffizienten a_{ij} von Q, wobei verschiedene Fälle zu unterscheiden sind. Wir gehen sofort von der äquivalenten Form Q_1 des Satzes 19 aus.

1. Wenn nicht alle $(r-1)$ reihigen Hauptminoren der Determinante a von Q_1 verschwinden, so können wir die x permutieren und annehmen, daß $A_{rr} \neq 0$. Dann erhalten wir die Form (30) mit $n = r$, von der also das Glied $\left(\frac{a}{A_{rr}}\right) x_r \tilde{x}_r$ abgespalten ist.

2. Wenn jedoch alle $(r-1)$ reihigen Hauptminoren verschwinden, so ist mindestens ein $A_{ij} \neq 0$, da der Rang r ist. Wieder darf man annehmen, daß $A_{r,r-1}$ dieses A_{ij} ist. Wir erhalten so die Form (33) mit $n = r$. Bei ihr sind zwei Glieder abgespalten.

Behandelt man den nichtreduzierten Teil — d. h. den unter dem Summationszeichen stehenden — in gleicher Weise, so erhält man schließlich die Form (34), in der die Koeffizienten Funktionen der Determinanten der Matrix von Q sind.

Ist z. B. die Voraussetzung 1. bei jedem Reduktionsschritt erfüllt, so hat die transformierte Form (34) die Koeffizienten

$$\frac{p_1}{p_0}, \frac{p_2}{p_1}, \frac{p_3}{p_2}, \ldots, \frac{p_{r-1}}{p_{r-2}}, \frac{p_r}{p_{r-1}} \qquad (p_i \neq 0), \tag{35}$$

wo $p_0 = 1$ und die übrigen p die Minoren aus (25) sind.

40. Größe des Index in der kanonischen Form. Wir hatten in 36. gezeigt, daß der Index einer kanonischen Form (17) eindeutig bestimmt ist. Um ihn zu finden, mußten wir jedoch diese kanonische Form herstellen. Es soll nun gezeigt werden, daß man den Index auch von vornherein angeben kann, ohne auf die kanonische Form zurückzugreifen. Ähnlich wie es zur Bestimmung der Rangzahl r auch nicht nötig war, die Form (15) herzustellen.

Nach Satz 18 können die Variabeln von Q so permutiert werden, daß $p_r \neq 0$ und keine zwei aufeinanderfolgenden der Zahlen (25) verschwinden. Wir nennen eine solche Form regulär.

Ist Q eine quadratische Form, so wird der Körper K als reell vorausgesetzt. Ist Q jedoch eine Hermitesche Form, so entstehe K aus einem reellen Körper S durch Adjunktion von $\sqrt{\nu}$, wo ν in S liegt und negativ ist. Für $x = a + b\sqrt{\nu}$, wo a und b in S liegen, ist dann $x\tilde{x} = a^2 - \nu b^2 > 0$, ausgenommen wenn $x = 0$. Auf

Digitized by Google Original from UNIVERSITY OF MICHIGAN

jeden Fall ist $p_i = \tilde{p}_i$ reell, und daher haben die beiden abgespaltenen Glieder von (33) entgegengesetztes Vorzeichen.

Nun bezeichne N die Zahl der Zeichenwechsel, P die der Zeichenfolgen in $p_0, p_1, \ldots, p_r$. Dabei muß ein verschwindendes p_i mitgezählt werden, allerdings mit beliebigem Vorzeichen.

Desgleichen bezeichne p die Zahl der positiven, n die Zahl der negativen Koeffizienten in der äquivalenten Form (34).

Sind nun alle $p_i \neq 0$, so sind diese Koeffizienten durch (35) gegeben. Für jede Zeichenfolge (-wechsel) haben zwei aufeinanderfolgende p gleiches (entgegengesetztes) Vorzeichen, und ihr Quotient ist eine der positiven (negativen) Zahlen von (35), und umgekehrt. In diesem Falle ist demnach $p = P$ und $n = N$.

Es läßt sich vermuten, daß dieses Resultat auch noch im Falle, wo eines der p, etwa p_i, verschwindet, richtig bleibt. — Zunächst sind dann, da Q regulär ist, $p_{i-1} \neq 0$ und $p_{i+1} \neq 0$. Setzt man in (32) $n = i + 1, a = p_{i+1}, b = p_{i-1}, A_{nn} = p_i$, so sieht man, daß p_{i-1} und p_{i+1} verschiedenes Vorzeichen haben. Wegen der beiden letzten Glieder von (33) haben wir jetzt an Stelle der beiden p_i enthaltenden Glieder in (35) zwei Koeffizienten von entgegengesetztem Vorzeichen. Da für die Sequenz $p_{i-1}, p_i = 0, p_{i+1}$ die Zeichen $+ \pm -$ oder $- \pm +$ sind, so ist für sie $P = N = 1$. Mit anderen Worten: lassen wir die Zeichenfolgen und -wechsel der Sequenz dieser drei Glieder außer Betracht, so erniedrigt sich P, N, p und n jedesmal um 1. Sind auf diese Art alle verschwindenden p getilgt, so gilt, wie wir sahen, für die übrigbleibenden, daß $p = P, n = N$. Dieselbe Beziehung bestand also auch vor der Tilgung.

Satz 22: In jedem reellen Körper ist jede quadratische Form vom Range r einer Form vom Typus $g_1 x_1^2 + \cdots + g_r x_r^2$ *äquivalent. Im einem Körper, der aus einem reellen Körper S durch Adjunktion der Quadratwurzel einer negativen Zahl aus S entsteht, ist jede Hermitesche Form vom Range r einer Form vom Typus* $g_1 x_1 \bar{x}_1 + \cdots + g_r x_r \bar{x}_r$, *wo alle g in S liegen, äquivalent. Die Zahl der positiven g ist die Zahl der Zeichenfolgen in* $p_0, p_1, \ldots, p_r$, *von denen keine zwei aufeinanderfolgenden verschwinden.*

Sei z. B. $Q = x_1^2 + 2x_2x_3 + x_4^2$. Dann ist $p_0 = 1$, $p_1 = 1$, $p_2 = 0$, $p_3 = p_4 = -1$, $P = 3$, $N = 1$. Und da Q äquivalent mit $x_1^2 + 2(\xi^2 - \eta^2) + x_4^2$, so ist in der Tat $p = 3$, $n = 1$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

FÜNFTES KAPITEL.

THEORIE DER LINEAREN TRANSFORMATIONEN. INVARIANTE FAKTOREN UND ELEMENTARTEILER.

Wir werden hier eine Einführung in die Theorie der Weierstraßschen Elementarteiler und der damit verwandten invarianten Faktoren geben. Wir werden diese Theorie in Verbindung mit der klassischen und einer neuen rationalen kanonischen Form einer linearen Transformation entwickeln.

41. Die rationale kanonische Form einer linearen Transformation.[1]) Ein wichtiger Gesichtspunkt der Untersuchungen der modernen Mathematik besteht darin, diejenigen Eigenschaften des zu untersuchenden Gegenstandes festzustellen, die sich bei gewissen Transformationen der Variabeln nicht ändern, die sich ihnen gegenüber also invariant verhalten. So ist es die Aufgabe der Invariantentheorie, die invarianten Funktionen der Koeffizienten und Variabeln einer Form zu untersuchen. Insbesondere hatten wir uns im ersten und zweiten Kapitel mit der Untersuchung der projektiven Invarianten beschäftigt, d. h. mit denjenigen Funktionen, die bei linearer Transformation der ursprünglichen Variabeln sich bei einem numerischen Faktor reproduzieren. — Im vierten Kapitel hatten wir gesehen, daß der Rang einer quadratischen Form sich gegenüber linearen Transformationen (mit $\Delta \neq 0$) der Variabeln invariant verhält, desgleichen der Index einer quadratischen usw. Form gegenüber gewissen linearen Transformationen.

---

1) Betr. des Falles, wo die Determinante nicht verschwindet, vergleiche man S. Lattès, Annales Fac. Sc. Toulouse (3), 6, 1914, pp. 1—84. Desgl. W. Krull, Über Begleitmatrizen und Elementarteiler, Freiburg, Dissertation, 1921. In den Leipziger Berichten 69, 1917, pp. 325—35, verwendet Gerh. Kowalewski Punkte anstatt der linearen Funktionen und erhält eine kanonische Form, deren Matrix die Transponierte von der im Texte erwähnten ist. — Die vorliegende Darstellung enthält die von dem Verfasser vor einigen Jahren gefundene Theorie.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

In diesem Kapitel soll nun unsere Aufgabe sein festzustellen, was bei der Matrix einer linearen Transformation selbst erhalten bleibt, wenn man die Variabeln der Transformation einer neuen Transformation unterwirft.

Dazu wollen wir zunächst die lineare Transformation auf eine kanonische Form bringen.

$w_1, \ldots, w_n$ seien unabhängige Variabeln. S sei eine lineare Transformation mit Koeffizienten aus K:

$$S: \quad W_i = \sum_{j=1}^{n} a_{ij} w_j \qquad (i = 1, \ldots, n).$$

Der Fall, bei dem die Determinante von S verschwindet, soll dabei nicht ausgeschlossen werden, so daß also die Matrix von S ganz allgemein ist.

x_1 sei eine beliebige homogene lineare Funktion von $w_1, \ldots, w_n$, deren Koeffizienten zu K gehören und nicht alle verschwinden. X_1 bedeute dieselbe Funktion von $W_1, \ldots, W_n$. Sind X_1 und x_1 in K linear abhängig, so besteht eine Beziehung von der Gestalt (1), wo dann $a = 1$ zu setzen ist, so daß nur die letzte Gleichung übrig bleibt. Sind aber X_1 und x_1 in K unabhängig, so schreibe man x_2 anstatt X_1 und bezeichne mit X_2 dieselbe Funktion der W_i, wie es x_2 von w_i ist. Ist jetzt X_2 von x_1 und x_2 abhängig, so besteht die Beziehung (1) mit $a = 2$, im entgegengesetzten Fall schreibe man x_3 anstatt X_2 und hat so drei linear unabhängige Funktionen x_1, x_2, x_3. Geht man auf diese Weise weiter, so erhält man eine Kette von linear unabhängigen Funktionen $x_1, x_2, \ldots, x_a$ mit Koeffizienten aus K, zwischen denen nach S die Beziehungen bestehen

$$(1) \quad X_1 = x_2, \quad X_2 = x_3, \ldots, \quad X_{a-1} = x_a, \quad X_a = [x_1, \ldots, x_a],$$

wobei die Klammer eine lineare homogene Funktion von $x_1, \ldots, x_a$ mit Koeffizienten in K bedeutet. Wir nennen a die Länge der Kette und x_1 ihr Leitglied. Nunmehr gilt der Satz:

Satz 1: Durch Einführung neuer Variabeln, welche unabhängige homogene lineare Funktionen der Ausgangsvariabeln w_i mit Koeffizienten aus K sind, läßt sich jede lineare Transformation S mit Koeffizienten aus K auf eine kanonische Form bringen, die durch (1) *und durch*

$$(2) \quad Y_1 = y_2, \quad Y_2 = y_3, \ldots, \quad Y_{b-1} = y_b, \quad Y_b = [y_1, \ldots, y_b],$$

$$(3) \quad Z_1 = z_2, \quad Z_2 = z_3, \ldots, \quad Z_{c-1} = z_c, \quad Z_c = [z_1, \ldots, z_c],$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

usw. definiert ist. Dabei bedeutet a die Maximallänge aller möglichen Ketten, b die Maximallänge einer Kette, deren Leitglied von $x_1, \ldots, x_a$ *linear unabhängig ist, und c die Maximallänge einer Kette, deren Leitglied linear ist unabhängig von* $x_1, \ldots, x_a, y_1, \ldots, y_b$.

Für $a = 1$ hat S die Form $W_i = a_{ii} w_i$ $(i = 1, \ldots, n)$, seine kanonische Form besitzt daher n Ketten. Es sei also $a > 1$. Man wähle eine Funktion x_1, welche das Leitglied einer Kette von der Maximallänge a ist, so daß die Beziehung (1) besteht. Ist $n = a$, so ist der Satz bewiesen.

Es sei also $n > a$. Mit u_1 bezeichne man eine beliebige homogene lineare Funktion der Ausgangsvariabeln w_i mit Koeffizienten aus K, welche von $x_1, \ldots, x_a$ linear unabhängig ist. U_1 bezeichne die gleiche Funktion der W_i. Sollte $U_1 = [x_1, \ldots, x_a, u_1]$ sein, so besteht (4) für $b = 1$. Andernfalls schreibe man u_2 für U_1. Ist nunmehr $U_2 = [x_1, \ldots, x_a, u_1, u_2]$, so besteht (4) für $b = 2$. Andernfalls schreibe man u_3 für U_2 usw. Auf diese Weise erhält man

$$(4) \quad U_1 = u_2, U_2 = u_3, \ldots, U_{b-1} = u_b, U_b = l + [u_1, \ldots, u_b],$$

wo $l = [x_1, \ldots, x_a]$ und $x_1, \ldots, x_a, u_1, \ldots, u_b$ linear unabhängig sind. Ist nun $l \equiv 0$, so haben wir in (4) schon das gewünschte Resultat (2), wenn wir $y_i = u_i$ setzen.

Es sei also $l \not\equiv 0$. Dann ist $l + [u_1, \ldots, u_b]$ linear unabhängig von $u_1, \ldots, u_b$, so daß u_1 das Leitglied einer Kette ist, dessen Länge größer als b ist. Es ist daher $b < a$. Führen wir die neuen Variabeln

$$y_1 = u_1 + f, y_2 = u_2 + f_1, \ldots, y_b = u_b + f_{b-1}$$

ein (wo f eine lineare homogene Funktion von $x_1, \ldots, x_a$ mit Koeffizienten aus K ist und wo f durch S in f_1, f_1 in f_2 usw. übergeht), so können wir f, wie unten gezeigt werden soll, so wählen, daß sich die Beziehung (2) ergibt.[1])

Um die dritte Kette zu erhalten, nehmen wir eine lineare homogene Funktion v_1 der Variabeln w_i mit Koeffizienten aus K, welche von $x_1, \ldots, x_a, y_1, \ldots, y_b$ linear unabhängig ist. V_1 bezeichne die entsprechende Funktion der W_i. Ist

$$V_1 = [x_1, \ldots, x_a, y_1, \ldots, y_b, v_1],$$

1) Der Beweis ist nämlich derselbe wie der von (6). Man hat dort nur die y fortzulassen und die z durch die y und c durch b zu ersetzen. Wir lassen an dieser Stelle die Einzelheiten daher weg und behandeln lieber die typische Ableitung der dritten Kette etwas ausführlicher.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

so besteht (5) für $c = 1$. Andernfalls schreibe man v_2 anstatt V_1. Ist jetzt $V_2 = [x_1, \ldots, x_a, y_1, \ldots, y_b, v_1, v_2]$, so besteht (5) für $c = 2$. Andernfalls schreibe man v_3 für V_2 und fahre in dieser Weise fort. So erhält man

$$(5) \qquad V_1 = v_2,\ V_2 = v_3, \ldots,\ V_{c-1} = v_c,\ V_c = l + m,$$

wo $\quad l = [x_1, \ldots, x_a, y_1, \ldots, y_b], \quad m = s_1 v_1 + \cdots + s_c v_c.$

Hier sind $x_1, \ldots, x_a, y_1, \ldots, y_b, v_1, \ldots, v_c$ linear unabhängig, und die s_i sind Zahlen aus K. Ist nun $l \equiv 0$, so ist (5) schon das gewünschte Resultat (3), wenn wir $z_i = v_i$ setzen.

Ist aber $l \not\equiv 0$, so ist jedenfalls $l + m$ linear unabhängig von $v_1, \ldots, v_c$, so daß v_1 das Leitglied einer Kette ist, deren Länge größer ist als c. Da aber v_1 linear unabhängig von $x_1, \ldots, x_a$ und da b die Maximallänge einer Kette ist, deren Leitglied unabhängig ist von $x_1, \ldots, x_a$, so haben wir $c < b$. — Nunmehr führen wir die neuen Variabeln

$$(6) \qquad z_1 = v_1 + f,\ z_2 = v_2 + f_1, \ldots, z_c = v_c + f_{c-1}$$

ein, wo $f = f_0$ eine homogene lineare Funktion von $x_1, \ldots, x_a, y_1, \ldots, y_b$, mit Koeffizienten aus K ist, während f_1 aus f, f_2 aus f_1 usw. durch die Transformation S entsteht. Wieder bezeichne Z_i dieselbe Funktion der W_i, wie z_i von w_i ist. Dann folgt aus (6), daß

$$(7) \qquad Z_1 = z_2,\ Z_2 = z_3, \ldots, Z_{c-1} = z_c,\ Z_c = l_1 + \sum_{i=1}^{c} s_i z_i,$$

wo $$l_1 = l + f_c - \sum_{i=1}^{c} s_i f_{i-1}.$$

Hier können wir nun f so wählen, daß l_1 eine homogene lineare Funktion der x_i, y_i $(i = 1, \ldots, c)$ wird. Der Beweis wird einfacher, wenn wir schrittweise vorgehen. Ist zunächst k der Koeffizient von x_a in l, so nehmen wir $f = -k x_{a-c}$, so daß $f_c = -k x_a$ wird und daher x_a in l_1 gar nicht mehr vorkommt. Da (7) und (5) dieselbe Gestalt haben, so können wir annehmen, daß l selbst von x_a frei ist. Ist nun t der Koeffizient von x_{a-1} in l, so setzen wir $f = -t x_{a-c-1}$, so daß $f_c = -t x_{a-1}$ wird und daher l_1 sowohl von x_{a-1} als x_a frei ist. Beim letzten dieser Schritte setzen wir, um x_{c-1} aus l_1 herauszuschaffen, $f = -g x_1$. — Ähnlich können wir die Koeffizienten von $y_{b-c}, y_{b-c-1}, \ldots, y_1$ in f so wählen, daß $y_b, y_{b-1}, \ldots, y_{c+1}$ aus l_1 verschwinden.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ist nun die sich ergebende Funktion $l_1 \equiv 0$, so ist (7) das verlangte Resultat (3). Im Gegenfall setze man

$$l_i = t_1 x_i + \cdots + t_c x_{c+i-1} + m_1 y_i + \cdots + m_c y_{c+i-1} \quad (i = 1, \ldots, b-c+1).$$

Da wir soeben bewiesen, daß l_1 durch diese Formel gegeben wird, wenn wir $i = 1$ setzen, so können die t und m nicht alle verschwinden. Bezeichnet L_i die entsprechende Funktion der X und Y, so ist daher

$$L_i = l_{i+1} \qquad (i = 1, \ldots, b-c). \tag{8}$$

Offenbar sind die l_i $(i = 1, \ldots, b-c+1)$ linear unabhängige Funktionen von x_j, y_j $(j = 1, \ldots, b)$. Nach (7) und (8) hat die Kette mit dem Leitglied z_1 die Glieder

$$z_1, \ldots, z_c, z_{c+j} = l_j + \sum_{i=1}^{c} s_i z_{i+j-1} \quad (j = 1, \ldots, b-c+1)$$

und vielleicht noch weitere Glieder. Nach (6) sind die $b+1$ Glieder z linear unabhängig. Da andererseits das Leitglied z_1 unabhängig von $x_1, \ldots, x_a$ ist, so widerspricht dieses Resultat der Definition von b.

42. Satz 2: Bei einer kanonischen Transformation ist die charakteristische Determinante der Teiltransformation jeder Kette ein Teiler derjenigen der vorhergehenden Kette.

Wir greifen den Fall, wo es sich um die zweite und dritte Kette handelt, heraus. Die Teiltransformationen sind dann

$$Y_1 = y_2, \; Y_2 = y_3, \ldots, Y_{b-1} = y_b, \; Y_b = \sum_{i=1}^{b} b_i y_i, \tag{9}$$

$$Z_1 = z_2, \; Z_2 = z_3, \ldots, Z_{c-1} = z_c, \; Z_c = \sum_{i=1}^{c} c_i z_i, \tag{10}$$

wo $c \leqq b$. Wir führen noch die linearen Funktionen

$$z_{c+1} = Z_c, z_{c+2} = Z_{c+1}, \ldots, z_{b+1} = Z_b \tag{11}$$

ein, welche sich vermöge der Rekursionsformel

$$z_{c+j} = \sum_{i=1}^{c} c_i z_{i+j-1} \qquad (j = 1, \ldots, b-c+1) \tag{12}$$

durch $z_1, \ldots, z_c$ ausdrücken lassen. — Die Kette mit dem Leitglied $w_1 = y_1 + z_1$ hat als Glieder die Funktionen $w_j = y_j + z_j$ $(j = 1, \ldots, b)$, welche linear unabhängig sind, da es auch $y_1, \ldots, y_b$,

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$z_1, \ldots, z_c$ sind. Da b die Maximallänge einer Kette mit einem von $x_1, \ldots, x_a$ unabhängigen Leitgliede ist, so ist die zu w_1 gehörende Kette von der Länge $\leqq b$, also gleich b. Man setze $W_j = Y_j + Z_j$. Dann ist

$$W_b = \sum_{i=1}^{b} b_i y_i + z_{b+1} = [w_1, \ldots, w_b]$$

$$= \sum_{i=1}^{b} b_i w_i = \sum_{i=1}^{b} b_i (y_i + z_i), \qquad \text{d. h.}$$

$$z_{b+1} = \sum_{i=1}^{b} b_i z_i. \tag{13}$$

Ist nun $c = b$, so ist nach (10) oder (12) $z_{b+1} = \sum c_i z_i$, also $c_i = b_i$. Es haben daher (9) und (10) dieselbe charakteristische Determinante.

Ist jedoch $c < b$, so können wir aus der Differenz der beiden Glieder von (13) $z_{b+1}, z_b, \ldots, z_{c+1}$ vermittels (12) eliminieren und erhalten eine lineare Funktion von $z_1, \ldots, z_c$, deren Koeffizienten sämtlich verschwinden müssen. Durch einen einfachen Bezeichnungswechsel sehen wir dann, daß, wenn wir $\lambda^{b+1}, \lambda^b, \ldots, \lambda^{c+1}$ aus

$$\lambda^{b+1} - \sum_{i=1}^{b} b_i \lambda^i \qquad \text{vermöge} \tag{14}$$

$$\lambda^{c+j} = \sum_{i=1}^{c} c_i \lambda^{i+j-1} \qquad (j = 1, \ldots, b-c+1) \tag{15}$$

eliminieren, wir eine lineare Funktion von $\lambda, \ldots, \lambda^c$ erhalten, deren Koeffizienten alle verschwinden. Diese Eliminationen sind aber offenbar nichts anderes als die einzelnen Schritte bei der gewöhnlichen Division von (14) durch

$$\lambda^{c+1} - \sum_{i=1}^{c} c_i \lambda^i. \tag{16}$$

Daher ist (14) durch (16) ohne Rest teilbar. Unterdrückt man bei beiden einmal den Faktor λ, so erhalten wir — abgesehen vom Vorzeichen — die charakteristischen Determinanten von (9) bzw. (10). Denn wenn N die Matrix von (9) bezeichnet, so ist ihre λ-Matrix $N - \lambda E$ gleich

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

$$(17) \qquad \begin{pmatrix} -\lambda & 1 & 0 & 0 \dots 0 \\ 0 & -\lambda & 1 & 0 \dots 0 \\ \cdot & \cdot & \cdot & \cdot \dots \cdot \\ b_1 & b_2 & b_3 & b_4 \dots b_b - \lambda \end{pmatrix},$$

also ihre Determinante, die sog. charakteristische Determinante von N, gleich

$$(18) \qquad (-1)^b (\lambda^b - b_1 - b_2\lambda - b_3\lambda^2 - \cdots - b_b\lambda^{b-1}).$$

Beispiel 1: S sei gegeben durch $W_1 = aw_1 + bw_2$, $W_2 = w_1$, $W_3 = bw_2 + aw_3$. Führen wir die neuen Variabeln $x_1 = w_2$, $x_2 = w_1$, $y = w_3 - w_1$, $X_1 = W_2$, usw. ein, so erhalten wir

$$C: \quad X_1 = x_2, \quad X_2 = bx_1 + ax_2, \quad Y = ay.$$

Scheinbar erhalten wir eine kanonische Form, die aus einer Kette x_1, x_2 und aus einer Kette y besteht. Die charakteristische Determinante der Teiltransformation von x_1 und x_2, d. h. $\lambda^2 - a\lambda - b$, ist aber nur dann durch die charakteristische Determinante $a - \lambda$ von $Y = ay$ teilbar, wenn $b = 0$. Ist b wirklich Null, so ist C die wahre kanonische Form von S, da jede lineare Funktion L von x_1, x_2, y das Leitglied einer Kette von der Länge 2 ist. Eine Ausnahme bildet nur der Fall, daß x_1 in L gar nicht vorkommt oder daß $L = k(x_2 - ax_1)$. In diesen beiden Fällen ist nämlich L das Leitglied einer Kette von der Länge 1. — Ist jedoch $b \neq 0$, so setze man

$$z_1 = x_1 + y, \quad Z_1 = X_1 + Y = x_2 + ay \equiv z_2,$$
$$Z_2 = X_2 + aY = bx_1 + ax_2 + a^2y \equiv z_3.$$

Die Determinante der Koeffizienten von x_1, x_2, y ist $-b$. Eine wahre kanonische Form im Falle $b \neq 0$ ist daher

$$Z_1 = z_2, \quad Z_2 = z_3, \quad Z_3 = -abz_1 + (b - a^2)\, z_2 + 2az_3.$$

Beispiel 2: Die kanonische Form von

$$W_1 = w_2 + w_3, \quad W_2 = w_1 + w_3, \quad W_3 = w_1 + w_2 + w_3$$

besitzt nur eine einzige Kette mit dem Leitgliede $x_1 = w_1$.

43. Satz 3: Es liege eine kanonische Transformation mit der n reihigen λ-Matrix M vor. $d_1, \dots, d_k$ seien die charakteristischen Determinanten der Teiltransformationen der Variabeln der 1ten, . . ., $k$ten Kette. g_i bezeichne den größten gemeinsamen Teiler aller $(n-i)$reihigen Determinanten von M. Dann ist

$$g_1 = d_2 \dots d_k, \; g_2 = d_3 \dots d_k, \dots, g_{k-1} = d_k, \; g_j = 1 \; (j \geq k).$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Wir schreiben M der Abkürzung halber in der Form

$$M = \begin{pmatrix} A_1 & 0 & 0 \dots 0 & 0 \\ 0 & A_2 & 0 \dots 0 & 0 \\ \cdot & \cdot & \cdot \cdot \cdot \cdot & \cdot \\ 0 & 0 & 0 \dots 0 & A_k \end{pmatrix},$$

wo man $A_1, \dots, A_k$ durch die λ-Matrizen der Teiltransformationen und die einzelnen Nullen durch entsprechend gewählte Nullmatrizen zu ersetzen hat. Z. B. ist A_2 durch (17) gegeben. Die Determinanten von $A_1, \dots, A_k$ sind $d_1, \dots, d_k$, ihre Elemente seien mit $a_{ij}, b_{ij}, \dots$ bezeichnet.

Der Minor M' irgendeines der Elemente der Nullmatrizen von M ist nun gleich Null. Denn angenommen, der Minor M' entstehe durch Tilgung einer Spalte, welche Elemente von A_1 enthält, und durch Tilgung einer Zeile, welche jedoch keine Elemente von A_1 enthält, so hat offenbar jeder a reihige Minor, der aus den ersten a Zeilen von M' gebildet wird, eine Spalte mit lauter Nullen. Demnach liefert die Laplacesche Zerlegung nach den ersten a Zeilen für M' den Wert Null.

Untersuchen wir nun die übrigen Minoren von M: Der Minor von b_1 in (17) ist 1, ebenso der von a_{a1} in A_1. Daher hat der Minor von a_{a1} in M die Form $g_1 = d_2 d_3 \cdots d_k$, während der Minor jedes anderen Elementes a_{ij} offenbar ein Vielfaches von g_1 ist. Ähnlich ist der Minor irgendeines b_{ij} ein Vielfaches von $d_1 d_3 \cdots d_k$, also auch von g_1, da d_1 nach Satz 2 ein Vielfaches von d_2 ist. Der Minor von c_{ij} ist ein Vielfaches von $d_1 d_2 d_4 \cdots d_k$, also auch von g_1. — So ergibt sich, daß g_1 größter gemeinsamer Teiler aller $(n-1)$ reihigen Minoren von M ist.

Gehen wir zu den $(n-2)$ reihigen Minoren von M über, so sehen wir ähnlich wie oben, daß diejenigen Minoren verschwinden, die man durch Tilgung zweier innerhalb einer Nullmatrix sich kreuzenden Zeilen und Spalten erhält. Der Minor, den man aus M erhält, wenn man die in a_{a1} sich kreuzende Zeile und Spalte sowie die in b_{b1} sich kreuzende Zeile und Spalte tilgt, ist offenbar $g_2 = d_3 \cdots d_k$, während der Minor, den man durch Tilgung der in a_{ij} und b_{mn} sich kreuzenden Zeilen und Spalten erhält, ein Vielfaches von g_2 ist. Desgleichen ist der zu a_{ij} und c_{mn} gehörige Minor ein Vielfaches von $d_2 d_4 \cdots d_k$, also auch von g_2.

Geht man auf diese Weise weiter, so gelangt man zu Satz 3.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

44. Invariante Faktoren einer kanonischen Transformation.

Nach (18) haben wir

(19) $d_1 = (-1)^a I_n,\ d_2 = (-1)^b I_{n-1}, \ldots, d_k = (-1)^e I_{n-k+1},$

wo $I_n, \ldots, I_{n-k+1}$ Polynome in λ sind, dessen höchste Potenz den Koeffizienten 1 hat. Man setzt noch, um immer dieselbe Zahl n von invarianten Faktoren zu haben,

(19′) $$I_{n-k} = 1, \ldots, I_1 = 1$$

und nennt jetzt allgemein I_j den $j$ten invarianten Faktor der λ-Matrix der kanonischen Transformation C. Abgesehen vom Vorzeichen sind die (von 1 verschiedenen) invarianten Faktoren die charakteristischen Determinanten der einzelnen Teiltransformationen.

Satz 4: Bezeichnet I_j den $j$ten invarianten Faktor der $n$reihigen λ-Matrix M einer kanonischen Transformation, so ist I_j in I_{j+1} als Teiler enthalten. Ist G_j der größte gemeinsame Teiler aller $j$reihigen Determinanten von M — das Leitglied in G_j muß dabei gleich 1 sein —, so ist nach Satz 2

(20) $$G_j = I_1 I_2 \ldots . I_j \qquad (j = 1, \ldots, n)\ (G_0 = 1),$$

(21) $$I_j = \frac{G_j}{G_{j-1}} \qquad (j = 1, \ldots, n),$$

so daß die G und I einander eindeutig bestimmen.

45. **Satz 5: Transformieren wir die Variabeln einer linearen Transformation A durch eine nichtsinguläre lineare Transformation B, so erhalten wir eine neue Transformation mit der „transformierten Matrix" $B^{-1}AB$.**

Denn eliminieren wir aus

$$A: \quad X_i = \sum_{j=1}^{n} a_{ij} x_j \qquad (i = 1, \ldots, n),$$

(22) $$B: \quad x_i = \sum_{k=1}^{n} b_{ik} y_k \qquad (i = 1, \ldots, n),$$

(23) $$B: \quad X_i = \sum_{k=1}^{n} b_{ik} Y_k \qquad (i = 1, \ldots, n),$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

wo $|b_{ik}| \neq 0$, die X_i und x_j, so erhalten wir wegen

$$B^{-1}: \quad Y_i = \sum_{m=1}^{n} c_{im} X_m \qquad (i = 1, \ldots, n)$$

die Transformation

$$B^{-1}AB: \quad Y_i = \sum_{m,j,k}^{1,\ldots,n} c_{im} a_{mj} b_{jk} y_k \qquad (i = 1, \ldots, n).$$

46. Drehungen und orthogonale Transformationen. Wir wollen die Einführung neuer Variabeln an einem wichtigen Beispiel erläutern. Es seien w_1, w_2, w_3 die Koordinaten eines willkürlichen Punktes W in bezug auf ein rechtwinkliges Koordinatensystem mit den Achsen Ow_1, Ow_2, Ow_3. Wir suchen die Koordinaten p_1, p_2, p_3 des Punktes P, der aus W durch eine Drehung um ON durch den Winkel α — und zwar im Uhrzeigersinn, wenn man von O nach N blickt — hervorgeht. Die Richtungskosinus von ON seien n_1, n_2, n_3. Wir wählen ein neues Koordinatensystem, dessen dritte Achse mit ON zusammenfällt, so daß die Richtungskosinus von Ox, Oy, Oz in bezug auf Ow_1, Ow_2, Ow_3 gleich l_1, l_2, l_3 bzw. m_1, m_2, m_3 bzw. n_1, n_2, n_3 sein mögen. In bezug auf diese neuen Achsen mögen W und P die Koordinaten x, y, z bzw. X, Y, Z haben. Dann ist also

$$(24) \quad X = x\cos\alpha - y\sin\alpha, \quad Y = x\sin\alpha + y\cos\alpha, \quad Z = z,$$

da wir in der Ebene arbeiten. Im Raume jedoch ist

$$(25) \quad \begin{aligned} x &= l_1 w_1 + l_2 w_2 + l_3 w_3, & w_1 &= l_1 x + m_1 y + n_1 z, \\ y &= m_1 w_1 + m_2 w_2 + m_3 w_3, & w_2 &= l_2 x + m_2 y + n_2 z, \\ z &= n_1 w_1 + n_2 w_2 + n_3 w_3, & w_3 &= l_3 x + m_3 x + n_3 z. \end{aligned}$$

Nun bezeichne man mit D die Determinante der durch das erste Tripel von Gleichungen definierten Transformation T. Das zweite Tripel definiert die inverse Transformation T^{-1}, deren Determinate man hier erhält, indem man in D Zeilen mit Spalten vertauscht. Infolgedessen ist $DD' = 1$, d. h. $D = \pm 1$. Man darf aber immer $D = +1$ voraussetzen, da man dies andernfalls durch Umkehren der Richtung einer der neuen Achsen erreichen kann. Löst man das zweite Tripel von Gleichungen nach z auf und vergleicht das Ergebnis mit $z = n_1 w_1 + \cdots$, so sieht man, daß

$$(26) \quad l_2 m_3 - l_3 m_2 = n_1, \quad l_3 m_1 - l_1 m_3 = n_2, \quad l_1 m_2 - l_2 m_1 = n_3.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Wir müssen nun die Transformation (24) durch die durch (25) definierten neuen Variabeln w_1, w_2, w_3 und durch

$$p_i = l_i X + m_i Y + n_i Z \qquad (i = 1, 2, 3)$$

ausdrücken. Dazu setzen wir in letzteren Ausdrücken die aus (24) und (25) sich ergebenden Werte ein und erhalten

$$p_i = \sum_{j=1}^{3} [(l_i l_j + m_i m_j) \cos \alpha + (l_j m_i - l_i m_j) \sin \alpha + n_i n_j] w_j .$$

Da für die Richtungskosinus zweier aufeinander senkrechter Geraden die Beziehung gilt, daß

$$\cos \varphi_1 \cdot \cos \psi_1 + \cos \varphi_2 \cdot \cos \psi_2 + \cos \varphi_3 \cdot \cos \psi_3 = 0 ,$$

so ist der Koeffizient von $\cos \alpha$ gleich $-n_i n_j$ bzw. $1 - n_i^2$, je nachdem $j \neq i$ oder $j = i$. Entsprechend ist der Koeffizient von $\sin \alpha$ gleich einem der Werte (26) oder gleich Null. Setzt man

$$a_0 = \cos \tfrac{1}{2}\alpha , \quad a_i = n_i \sin \tfrac{1}{2}\alpha \qquad (i = 1, 2, 3), \tag{27}$$

so ist wegen $\cos \alpha = 2a_0^2 - 1$ der Koeffizient von w_i in p_i gleich

$$(1 - n_i^2) \cos \alpha + n_i^2 = 2a_0^2 - 1 + 2\left(n_i \sin \tfrac{1}{2}\alpha\right)^2 .$$

Sodann ist für $j \neq i$ der Koeffizient von w_j gleich

$$n_i n_j (1 - \cos \alpha) + e_{ji} n_k \sin \alpha = 2 n_i n_j \sin^2 \frac{\alpha}{2} + 2 e_{ji} n_k \sin \frac{\alpha}{2} \cos \frac{\alpha}{2} ,$$

wo k die von i und j verschiedene Zahl 1, 2 oder 3 bezeichnet, während

$$e_{12} = e_{23} = e_{31} = +1 , \quad e_{13} = e_{21} = e_{32} = -1$$

ist. Setzt man die Werte aus (27) ein, so erhält man

$$p_i = (2a_0^2 - 1 + 2a_i^2) w_i + \sum_{j \neq i}^{1,2,3} [2 a_i a_j + 2 e_{ji} a_k a_0] w_j$$

oder in ausführlicher Schreibweise

$$\begin{aligned}
p_1 &= (2a_1^2 + 2a_0^2 - 1) w_1 + 2(a_1 a_2 - a_3 a_0) w_2 + 2(a_1 a_3 + a_2 a_0) w_3 , \\
p_2 &= 2(a_1 a_2 + a_3 a_0) w_1 + (2a_2^2 + 2a_0^2 - 1) w_2 + 2(a_2 a_3 - a_1 a_0) w_3 , \\
p_3 &= 2(a_1 a_3 - a_2 a_0) w_1 + 2(a_2 a_3 + a_1 a_0) w_2 + (2a_3^2 + 2a_0^2 - 1) w_3 .
\end{aligned} \tag{28}$$

Satz 6: Formel (28) *stellt die Drehung um die Achse ON mit den Richtungskosinus n_1, n_2, n_3 durch den Winkel α dar (die Drehungsrichtung ist, wenn man von O nach N blickt, im Sinne des Uhrzeigers).*

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Werte a_0, a_1, a_2, a_3 erfüllen nach (27) die Beziehung

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = 1.$$

Gehen wir nun von einer reellen ternären orthogonalen Vektortransformation T: $y_i = b_{i1}x_1 + b_{i2}x_2 + b_{i3}x_3$ $(i = 1, 2, 3)$

(vgl. 37.) aus, deren Matrix B also die Determinante $+1$ hat, so daß $BB' = E$. Ist D die Determinante von $B - E$, also auch die von $B' - E$, so ist

$$B'(B - E) = -(B' - E), \quad |B'|D = -D,$$

d. h. $D = 0$. — Nun ist der Vektor $N = (n_1, n_2, n_3)$ ein Ruhevektor gegenüber T, wenn

$$n_i = b_{i1}n_1 + b_{i2}n_2 + b_{i3}n_3 \qquad (i = 1, 2, 3).$$

Diese Gleichungen haben nun nichttriviale Lösungen, da ihre Determinante $D = 0$. Der Vektor $X = (x_1, x_2, x_3)$ möge durch T in $Y = (y_1, y_2, y_3)$ übergehen. Dann ist wegen

$$y_i - n_i = b_{i1}(x_1 - n_1) + b_{i2}(x_2 - n_2) + b_{i3}(x_3 - n_3)$$

$\sum(y_i - n_i)^2 = \sum(x_i - n_i)^2$, da $\sum y_i^2 = \sum x_i^2$ für T. Ist daher O der Ursprung, so ist $OY = OX$, $NX = NY$, so daß die Dreiecke OXN und OYN kongruent sind. X und Y liegen also auf einem Kreis, dessen Ebene senkrecht zu ON ist, so daß T eine Drehung um ON darstellt.

Eine orthogonale Transformation von der Determinante -1 ist offenbar das Produkt einer solchen von der Determinante $+1$ und der Spiegelung an der xy-Ebene, d. h. $X = x$, $Y = y$, $Z = -z$.

Satz 7: Jede reelle ternäre orthogonale Vektortransformation stellt eine Drehung dar oder eine Drehung verbunden mit einer Spiegelung, je nachdem ihre Determinante gleich $+1$ oder -1 ist.

Folgerung: Jede reelle orthogonale ternäre (Vektor-)Transformation mit der Determinante $+1$ wird durch die Formel (28) dargestellt.

Von den n^2 Koeffizienten einer $n$ären orthogonalen Transformation sind nur $\frac{n}{2}(n-1)$ wesentlich. Cayley[1]) hat die Koeffi-

1) In Pascals „Determinanten", §§ 47—50 finden sich die Namen von 20 Autoren angeführt, die sich mit orthogonalen Transformationen befaßt haben.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

zienten der Transformation durch diese Parameter ausgedrückt, ohne indessen damit alle Transformationen zu erhalten, vielmehr gingen ihm einige Grenzfälle verloren. — In 54., Beispiel 3—6 werden wir eine Darstellung aller Transformationen angeben.

Dieses Problem ist nur ein bestimmter Fall des allgemeineren aus der Theorie[1]) der linearen Transformationen, nämlich die automorphen linearen Transformationen einer quadratischen oder bilinearen Form anzugeben, d. h. diejenigen linearen Transformationen, welche die Form in sich selbst überführen.

47. *Satz 8: A bzw. B seien n-reihige quadratische Matrizen, deren Elemente Polynome in λ bzw. unabhängig von λ sind, und es sei $|B| \neq 0$. Dann haben die t-reihigen Determinanten von A und AB denselben größten gemeinsamen Teiler $D_t(\lambda)$, dessen Leitglied gleich eins ist.*

Nach Satz 5 von Kapitel III ist D_t durch d_t, den größten gemeinsamen Teiler aller $t$reihigen Determinanten von A, teilbar. Derselbe Satz zeigt aber auch, daß d_t durch D_t teilbar ist, da A das Produkt von AB und B^{-1} ist. Daraus folgt, daß $D_t = d_t$.

Da derselbe Satz auch für BA gilt, so erhalten wir die

Folgerung: A, P, Q seien $n$reihige quadratische Matrizen, und zwar seien die Elemente von A Polynome in λ, während die von P und Q von λ frei sind. Außerdem seien P und Q nichtsingulär. Dann haben die $t$reihigen Determinanten von A und PAQ denselben größten gemeinsamen Teiler.

48. Nehmen wir jetzt insbesondere A als die λ-Matrix einer linearen Transformation T an, so daß $A = T - \lambda E$. Durch die Einführung neuer Variabeln mittels der nichtsingulären Transformation B möge T in C übergehen, wo nach Satz 5 $C = B^{-1}TB$. Ferner ist $D = C - \lambda E = B^{-1}AB$. Nach unserer Folgerung haben also die t reihigen Determinanten von A und D dieselben größten gemeinsamen Teiler. D. h.:

Satz 9: Der größte gemeinsame Teiler G_t aller $t$reihigen Determinanten einer λ-Matrix bleibt bei Einführung neuer unabhängiger Variabeln ungeändert. Speziell ändert sich also die charakteristische Determinante nicht.

---

1) Vgl. Encyclopédie des sc. math., t. I, v. II, pp. 478—520. — Muth, Elementarteiler, 1899, pp. 160—179. — Betr. Hermitescher Formen vgl. Loewy, Nova Acta Leop. Carol. Akad. 71, 1898, pp. 379—416; im Auszug in den Mathem. Ann. 50, 1898, pp. 557—576.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Damit haben wir die im Anfang von 41. erwähnten Invarianten einer linearen Transformation gefunden.

49. Die eindeutige Bestimmtheit der kanonischen Form durch ihre invarianten Faktoren. Die neuen Variabeln seien so gewählt, daß C die kanonische Form von T ist. Da die λ-Matrizen dieser Transformationen dieselben G_t haben, so haben sie auch dieselben $I_j = \frac{G_j}{G_{j-1}}$, durch welche nach (19) die charakteristischen Determinanten der einzelnen Teiltransformationen von C eindeutig bestimmt sind.

Satz 10: Für jede lineare Transformation T ist der Quotient $I_j = \frac{G_j}{G_{j-1}}$ ein Polynom in λ und heißt der $j$te invariante Faktor von T. Die Matrix der kanonischen Form von T ist durch diese invarianten Faktoren eindeutig bestimmt. Die invarianten Faktoren ändern sich nicht bei linearer nichtsingulärer Transformation.

Jede lineare Transformation hat daher, abgesehen von der Bezeichnung der Variabeln, eine einzige kanonische Form. — Gleichzeitig ist so der Begriff der invarianten Faktoren auf alle Transformationen ausgedehnt worden, während er vorher auf kanonische Formen beschränkt war.

50. *Satz 11: I_j seien Polynome mit Koeffizienten aus einem Körper K von der Eigenschaft, daß I_j in I_{j+1} enthalten ist für alle j. Dann gibt es eine lineare Transformation mit Koeffizienten aus K, deren λ-Matrix die vorgeschriebenen Invarianten I_j besitzt.*

51. Ähnliche Transformationen. Zwei lineare Transformationen (oder Matrizen) S und T aus K heißen in K ähnlich, wenn es eine nichtsinguläre Transformation B aus K gibt, die S in T überführt, wenn also $B^{-1}SB = T$. Satz 9 zeigt dann, daß die λ-Matrizen zweier ähnlichen Transformationen dieselben G_t (und I_t) haben.

Indessen gilt auch die Umkehrung: Wenn die λ-Matrizen von S und T dieselben G_t haben, so sind S und T in K ähnlich. Denn wenn man die kanonischen Formen von S und T mit $U = Q^{-1}SQ$ und $V = R^{-1}TR$ bezeichnet, so sind die kanonischen Matrizen U und V nach Satz 10 identisch, da sie dieselben G_t besitzen. Es ist also

$$Q^{-1}SQ = V, \quad RVR^{-1} = T, \quad \text{d. h. } (QR^{-1})^{-1}S(QR^{-1}) = T,$$

so daß unsere Behauptung bewiesen ist.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 12: Lineare Transformationen (oder Matrizen) aus K sind dann und nur dann in K ähnlich, wenn ihre λ-Matrizen dieselben invarianten Faktoren haben.

52. Allgemeinere Definition der invarianten Faktoren. M und N seien zwei $n$reihige quadratische Matrizen, außerdem sei N nichtsingulär. Nach Satz 8 hat dann $M - \lambda N = (MN^{-1} - \lambda E)N$ dieselben G_i wie $MN^{-1} - \lambda E$. Für letztere ist $I_j = \frac{G_j}{G_{j-1}}$ ein Polynom in λ (vgl. Satz 10) und kann daher als der $j$te invariante Faktor von $M - \lambda N$ definiert werden.

Wir wollen jetzt die Beschränkung, daß N nichtsingulär sein soll, beseitigen. Dazu betrachten wir die $j$reihigen Determinanten von $\varrho M + \sigma N$, wo ϱ und σ unabhängige Variabeln sind. G_j sei der größte gemeinsame Teiler von diesen. Entwickelt man nun jede dieser $j$reihigen Determinanten nach den Elementen einer Zeile oder Spalte, so erhält man eine lineare Kombination gewisser $(j-1)$reihiger Determinanten von $\varrho M + \sigma N$, deren jede G_{j-1} als Faktor enthält. Der Quotient $\frac{G_j}{G_{j-1}}$ ist daher ein homogenes Polynom in ϱ und σ und heißt der $j$te invariante Faktor von $\varrho M + \sigma N$.

Übungen: 1. $X_1 = x_2$, $X_2 = a x_2$, $X_3 = a x_3$ hat die invarianten Faktoren $\lambda(\lambda - a)$, $\lambda - a$, 1.

2.
$$\begin{pmatrix} 0 & 0 & 2-\lambda \\ 0 & 1+\lambda & 2\lambda \\ 2-\lambda & 0 & 0 \end{pmatrix}$$
hat die invarianten Faktoren $(\lambda - 2)(1 + \lambda)$, $\lambda - 2$, 1.

53. Die klassische[1] kanonische Form. Die Koeffizienten unserer bisherigen kanonischen Form waren rationale Funktionen der Koeffizienten der Ausgangsform. Für manche Zwecke zieht man indessen eine kanonische Form vor, welche gewisse Irrationalitäten enthält. Sie soll nunmehr aufgestellt werden.

Satz 13: Wir gehen aus von unserer kanonischen Form mit Koeffizienten aus K, die also aus Teiltransformationen von dem Typus

$$(29) \quad X_1 = x_2, \quad X_2 = x_3, \ \ldots, \quad X_{a-1} = x_a, \quad X_a = \sum_{i=1}^{a} a_i x_i$$

1) Jordan (Traité des Substitutions, 1870, pp. 114—126) stellte den Satz nur für Transformationen mit ganzen Koeffizienten (modulo p) und einer zu p teilerfremden Determinante auf. — Für einen beliebigen Körper vgl. Dickson, Amer. Jour. Math. 24, 1902, pp. 101—108.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

besteht. Die charakteristische Determinante $\Delta(\lambda)$ von (29) *möge die Wurzeln $R, S, T, \ldots$ mit den Multiplizitäten $r, s, t, \ldots$ haben. Dann läßt sich* (29) *durch Einführung neuer linear unabhängiger homogener linearer Funktionen $u_i, v_i, w_i, \ldots$ von $x_1, \ldots, x_a$ auf die Gestalt*

$$(30)\qquad \begin{cases} U_1 = Ru_1, & U_j = Ru_j + u_{j-1} \quad (j=2,\ldots,r), \\ V_1 = Sv_1, & V_j = Sv_j + v_{j-1} \quad (j=2,\ldots,s), \\ W_1 = Tw_1, & W_j = Tw_j + w_{j-1} \quad (j=2,\ldots,t), \ldots \end{cases}$$

bringen. Hier sind die u_i (bzw. v_i, bzw. w_i) Funktionen der x mit Koeffizienten, welche Polynome in R (bzw. S, bzw. T) mit Koeffizienten aus K sind. Sind R und S Wurzeln derselben in K irreduziblen[1]*) Gleichung, so bekommt man v_i aus u_i, indem man R durch S ersetzt.*

Wir wollen zunächst beweisen, daß (29) und (30) im Körper aller komplexer Zahlen einander ähnlich sind, daß sie sich also ineinander transformieren lassen. Explizite Formeln für die $u_i, v_i, w_i, \ldots$ werden wir allerdings damit nicht gewinnen.

Die λ-Matrix der Transformation der ersten Zeile von (30) ist

$$A_1 = \begin{pmatrix} R-\lambda & 0 & 0 & \ldots & 0 & 0 & 0 \\ 1 & R-\lambda & 0 & \ldots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & 0 & 1 & R-\lambda \end{pmatrix}.$$

Ähnlich seien A_2 und A_3 die λ-Matrizen der Transformationen der zweiten und dritten Zeile von (30). Führt man diese Abkürzungen ein, so ist die λ-Matrix von (30)

$$M = \begin{pmatrix} A_1 & 0 & 0 & 0 & \ldots \\ 0 & A_2 & 0 & 0 & \ldots \\ 0 & 0 & A_3 & 0 & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

Unser vorläufiges Ziel ist, die invarianten Faktoren von M festzustellen. Nun ist die Determinante von A_1 gleich $d_1 = (R-\lambda)^r$, während der Minor des letzten Elementes der ersten Zeile von A_1 gleich 1 ist. Entsprechend sind die Determinanten von $A_2, A_3, \ldots$ gleich $d_2 = (S-\lambda)^s$, $d_3 = (T-\lambda)^t, \ldots$. Dann ist die Determinante von M gleich $\Delta = d_1 d_2 d_3 \ldots$, während $d_2 d_3 d_4 \ldots$, $d_1 d_2 d_3 \ldots$, $d_1 d_2 d_4 \ldots$ unter den ersten Minoren von M vor-

1) Über die Definition der Irreduzibilität siehe 82.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

kommen, da ja z. B. ein Minor von A_1 gleich eins ist. Der größte gemeinsame Teiler der Minoren von M ist demnach gleich 1, da er keinen der möglichen Faktoren $R-\lambda$, $S-\lambda, \ldots$, enthält. — Andererseits ist auch der größte gemeinsame Teiler der ersten Minoren der λ-Matrix von (29) gleich 1, da es Minoren gibt — ähnlich wie den von b_1 in (17) —, die gleich 1 sind. Die λ-Matrizen von (29) und (30) haben also dieselben invarianten Faktoren $1, 1, \ldots, 1, \pm \Delta$, sind demnach nach Satz 12 ähnlich. Mit anderen Worten: es gibt Variabeln, nach deren Einführung sich (29) auf (30) reduziert.

Der vorstehende Beweis ist ein Existenzbeweis, d. h. er zeigt nur, daß eine solche angegebene Darstellung möglich ist, gibt jedoch keine Mittel an die Hand, die Funktionen $u_i, v_i, w_i, \ldots$ wirklich zu berechnen. Dies soll nunmehr geschehen. Gleichzeitig sollen die übrigen am Ende von Satz 13 erwähnten Eigenschaften bewiesen werden. Letztere sind in den verschiedenartigsten Anwendungen von großer Wichtigkeit, indessen werden wir in diesem Buche weiter keinen Gebrauch davon machen, so daß der nicht interessierte Leser sich mit dem Existenzbeweis begnügen und daher die folgenden Entwicklungen übergehen kann.

Wir gehen wieder von (29), wo die a_i zu K gehören, aus. Wie in (18), so ist auch in (29) die charakteristische Determinante gleich $(-1)^a C_a(\lambda)$, wo

$$C_{a-k}(\lambda) \equiv \lambda^{a-k} - \sum_{i=0}^{a-k-1}{}' a_{i+k+1}\lambda^i \qquad (k = 0, 1, \ldots, a-1). \tag{31}$$

Definiert man $C_0(\lambda)$ als 1, so geht die Funktion

$$f(\lambda) \equiv \sum_{k=1}^{a} x_k C_{a-k}(\lambda)$$

vermöge (29) in $Q(\lambda) \equiv \sum_{j=2}^{a} x_j Q_j + a_1 x_1$ über, wo

$$Q_j \equiv C_{a-j+1}(\lambda) + a_j = \lambda^{a-j+1} - \sum_{i=0}^{a-j} a_{i+j}\lambda^i + a_j = \lambda C_{a-j}(\lambda).$$

Daher ist

$$Q(\lambda) - \lambda \cdot f(\lambda) \equiv x_1[a_1 - \lambda \cdot C_{a-1}(\lambda)] \equiv -x_1 C_a(\lambda), \tag{32}$$

wo die letzte Reduktion aus dem vorigen Ergebnis für $j = 1$ folgt. Durch $t$fache Differentiation nach λ erhalten wir

$$Q^{(t)}(\lambda) - tf^{(t-1)}(\lambda) - \lambda f^{(t)}(\lambda) \equiv -x_1 C_a^{(t)}(\lambda). \tag{33}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ist jetzt R eine Wurzel von $C_a(\lambda) = 0$ von der Multiplizität r, so schreibe man für $f(R)$ einfach u_1, für den Quotienten von $f^{(t)}(R)$ durch $t!$ kurz u_{t+1}.[1]) Da $f(\lambda)$ durch (29) in $Q(\lambda)$ und daher auch $f^{(t)}(\lambda)$ in $Q^{(t)}(\lambda)$ übergeht, so geht u_{t+1} in $Q^{(t)}(R)/t!$ über, welches wir demnach mit U_{t+1} bezeichnen. Setzt man nun in (32) und (33) $\lambda = R$, so erhalten wir

$$U_1 = Ru_1, \quad U_{t+1} = Ru_{t+1} + u_t \qquad (t = 1, \ldots, r-1),$$

was mit der ersten Zeile von (30) identisch ist, wenn man j an Stelle von $t + 1$ setzt. Ihrer Entstehung nach sind die u_i lineare Funktionen von $x_1, \ldots, x_a$, deren Koeffizienten Polynome in R mit Koeffizienten aus K sind.

Es ist jetzt nur noch zu beweisen, daß die neuen Variabeln in K unabhängig sind. Wenn also eine Beziehung der Form

$$\sum_{j=1}^{r} g_j u_j + \sum_{j=1}^{s} h_j v_j + \sum_{j=1}^{t} k_j w_j \equiv 0 \tag{34}$$

bestehen sollte, so haben wir zu zeigen, daß die Konstanten g, h, k alle verschwinden. In der entsprechenden Identität für die U, V, W setzen wir die Werte (30) ein, subtrahieren davon die mit R multiplizierte Gleichung (34) und erhalten

$$\sum_{j=2}^{r} g_j u_{j-1} + \sum_{j=1}^{s} h_j (S - R) v_j + \sum_{j=2}^{s} h_j v_{j-1} + \sum_{j=1}^{t} k_j (T - R) w_j + \sum_{j=2}^{t} k_j w_{j-1} \equiv 0. \tag{35}$$

Wenn wir nun beweisen können, daß die Koeffizienten von u_i, v_i, w_i in (35) alle verschwinden, so muß k_t als Koeffizient von w_t verschwinden, ferner k_{t-1} als der von $w_{t-1}, \ldots, k_1$ als der von w_1. Ähnlich ist jedes $h_i = 0$ und jedes $g_j = 0$ (für $j > 1$), so daß (34) in $g_1 u_1 = 0$ übergeht. Da aber der Koeffizient von x_a in $u_1 = f(R)$ gleich $C_0(R) = 1$ ist, so ist $g_1 = 0$, so daß auch in (34) alle Koeffizienten verschwinden.

Nun hat aber (35) dieselbe Gestalt wie (34), ist jedoch frei von u_r, es genügt daher zu beweisen, daß eine Beziehung der Form (34),

---

1) Die Division geht für jeden Koeffizienten auf. — Der ganze Beweis ist auch gültig, wenn K ein sog. Modulbereich ist, d. h. ein Bereich, in dem die $p$fache Addition jedes Elementes zu sich selbst auf die Null führt. Ein Beispiel bildet das Feld der Reste der ganzen Zahlen modulo (d. h. bei der Division durch) p.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

in der u_r gar nicht vorkommt, lauter verschwindende Koeffizienten hat. Die neue Identität (35) enthält jetzt weder u_r noch u_{r-1}. Setzt man sie an Stelle von (34), so reduziert sich das Problem durch Wiederholung dieser Schlußweise auf ein solches, in dem nur die v_i und w_i vorkommen. In die entsprechende Identität in V_i und W_i setzen wir die Werte (30) ein, subtrahieren davon die mit S multiplizierte frühere Identität und erhalten schließlich eine Beziehung in den w allein. Diesmal subtrahieren wir dann das Produkt mit T.

54. Elementarteiler. In der klassischen kanonischen Transformation (30) sind, wie wir sahen, die charakteristischen Determinanten der Teiltransformationen der einzelnen Zeilen von (30) gleich

$$(36) \qquad (\lambda - R)^r, \quad (\lambda - S)^s, \quad (\lambda - T)^t, \ldots$$

(abgesehen vom Vorzeichen). Ihr Produkt ist (abgesehen vom Vorzeichen) die charakteristische Determinante $\Delta(\lambda)$ von (29), also ihr einziger von 1 verschiedener invarianter Faktor. Die Divisoren (36) heißen die Elementarteiler von $\Delta(\lambda)$ oder der λ-Matrix von (29). Erinnert man sich der Definition (19) der invarianten Faktoren einer kanonischen linearen Transformation, von der unsere Transformation (29) nur eine Teiltransformation ist, so erhält man

Satz 14: Man greife aus jedem invarianten Faktor einer linearen Transformation die höchste in ihm enthaltene Potenz jedes seiner Linearfaktoren heraus. Sie bilden die Elementarteiler der λ-Matrix der linearen Transformation. — Umgekehrt erhalten wir aus den in beliebiger Reihenfolge angegebenen Elementarteilern die von 1 verschiedenen invarianten Faktoren I_j, wenn wir berücksichtigen, daß I_j in I_{j+1} enthalten ist.

Z. B. seien die invarianten Faktoren

$$I_1 = I_2 = \cdots = I_6 = 1, \quad I_7 = \lambda, \quad I_8 = \lambda(\lambda - 1)^2,$$
$$I_9 = \lambda^2(\lambda - 1)^3.$$

Dann sind die Elementarteiler gleich

$$\lambda^2, \lambda, \lambda, (\lambda - 1)^3, (\lambda - 1)^2.$$

Sind umgekehrt letztere gegeben, so erhält man I_9 als Produkt der höchsten Potenzen der verschiedenen linearen Funktionen, sodann I_8 als Produkt der nächst höheren Potenzen usw.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die klassische kanonische Form zeigt, daß eine lineare Transformation von n Variabeln existiert, deren λ-Matrix irgendwelche vorgeschriebenen Elementarteiler vom Gesamtgrade n enthält.

Unsere Definition der Elementarteiler gilt bis jetzt nur für die λ-Matrizen $M - \lambda N$. Sie läßt sich indessen leicht auf Matrizen der Form $P = \varrho M + \sigma N$ ausdehnen, wo M und N beliebige $n$reihige quadratische Matrizen sind. Denn die in 52. definierten (von 1 verschiedenen) invarianten Faktoren I_j von P lassen sich als Produkte von Potenzen von linearen Funktionen von ϱ und σ ausdrücken. Diese Potenzen heißen die Elementarteiler von P.

Aus Satz 10 folgt, daß sich auch die Elementarteiler gegenüber linearen Transformationen invariant verhalten. — Damit haben wir unser im Anfang von 41 aufgestelltes Ziel erreicht, nämlich Invarianten einer linearen Transformation gefunden: Die invarianten Faktoren sowie die Koeffizienten der charakteristischen Gleichung sind im Körper K ganz-rationale absolute Invarianten, die Elementarteiler hingegen irrationale absolute Invarianten.

Übungen: 1. Die kanonische lineare Transformation von drei Variabeln ist von einem der drei Typen

$$\begin{array}{lll} U = Ru, & V = Sv, & W = Tw; \\ U_1 = Ru_1, & U_2 = Ru_2 + u_1, & V = Sv; \\ U_1 = Ru_1, & U_2 = Ru_2 + u_1, & U_3 = Ru_2 + u_2. \end{array}$$

2. Bestimme die Elementarteiler der λ-Matrix jeder der Transformationen aus Beispiel 1.

3. Man bestätige, daß die Formel (28) für die Drehung einer Kugel auch durch die reelle Quaternionengleichung $p = qwq'$ dargestellt wird, wo

$$q = a_0 E + a_1 i + a_2 j + a_3 k, \quad w = w_1 i + w_2 j + w_3 k,$$
$$p = p_1 i + p_2 j + p_3 k$$

und q die Norm 1 hat. Vgl. Beispiel 6.

4. Die Gleichung $\xi = xy$ in den Matrizen

$$\xi = \begin{pmatrix} \xi_1 & \xi_2 \\ \xi_3 & \xi_4 \end{pmatrix}, \quad x = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \quad y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$$

definiert eine homogene lineare Transformation der $x_1, \ldots, x_4$, welche offenbar die durch $|x| = 0$ definierte quadratische Fläche S in sich selbst überführt. Man weise nach, daß sie jede der auf S gelegenen Geraden

$$L_k: \quad x_1 = k x_3, \quad x_2 = k x_4$$

unverändert läßt. Ähnlich wird durch $\xi = yx$ jede der Geraden

$$l_k: \quad x_1 = k x_2, \quad x_3 = k x_4$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

auf S in sich selbst transformiert. Daher läßt $\xi = z x y$ S unverändert und permutiert die Geraden L_k untereinander und ebenso die Geraden l_k. Es läßt sich zeigen, daß diese Transformationen sowie ihre Produkte mit $(x_3 x_3)$, welche die beiden Komplexe von Geraden vertauscht, die einzigen sind, welche S in sich selbst überführen (Dickson, Bull. Amer. Math. Soz. 22, 1915, pp. 53—61).

5. In Beispiel 4 führe man neue Variabeln X_r und Y_r ein, durch welche S in $\sum X_r^2 = 0$ übergeht:

$$x_1 = X_1 + iX_4, \quad x_4 = X_1 - iX_4, \quad x_2 = -X_2 + iX_3, \quad x_3 = X_2 + iX_3,$$

$$y_1 = Y_4 - iY_1, \quad y_4 = Y_4 + iY_1, \quad y_2 = Y_3 + iY_2, \quad y_3 = -Y_3 + iY_2.$$

Dann entspricht $\xi = xy$ der Quaternionengleichung $\Xi = XY$, wo $X = X_1 i + X_2 j + X_3 k + X_4 E$. Sind also Z und Y reelle Quaternionen, so liefert die Gleichung $\Xi = ZXY$ alle reellen linearen Transformationen mit positiver Determinante, welche $\sum X_r^2$ bis auf einen konstanten Faktor in sich selbst überführen.[1])

6. Man leite aus Beispiel 5 die reellen orthogonalen Transformationen dreier Variabeln her. Man setze also $X_4 = 0$, $\Xi_4 = 0$, so daß $X + X' = 0$, $\Xi + \Xi' = 0$. Es ist dann $ZXY = Y'XZ'$. Setzt man p für $Z'Y^{-1}$, so ist demnach $p'X = Xp$. Der Spezialfall $X = i$ zeigt, daß der Koeffizient von i in p verschwindet. Ebenso sind aus Gründen der Symmetrie die Koeffizienten von j und k in p gleich Null. Es ist daher $p = rE$, wo r reell ist. Demnach ist $Z' = rY$ und $\Xi = ZXZ'r^{-1}$. Nimmt man auf beiden Seiten die Norm, so sieht man, daß wegen der Invarianz von $X_1^2 + X_2^2 + X_3^2$ die Norm von Z gleich $\pm r$ sein muß. Für die reelle Quaternion $Z(\pm r)^{-\frac{1}{2}}$ mit der Norm 1 setze man q. Dann ist $\Xi = \pm qXq'$. Das Vorzeichen ist positiv oder negativ, je nachdem die Determinante der orthogonalen Transformation gleich $+1$ oder -1 ist. Daraus ergibt sich ein neuer Beweis von Beispiel 3.

---

1) Einen eleganten Beweis, der nur Quaternionen benutzt, gibt Hurwitz in seiner „Zahlentheorie der Quaternionen", Berlin 1919, pp. 62—66.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

SECHSTES KAPITEL.

PAARE VON BILINEAREN UND QUADRATISCHEN FORMEN.

55. Historisches. Die erste Theorie der Paare bilinearer und quadratischer Formen (deren zweite jedesmal nichtsingulär war) stammt von Weierstraß[1]), der dazu Reihenentwicklungen, in denen gewisse Quadratwurzeln vorkommen, benutzte. Doch befand sich in seinem Beweis eine große Lücke. Für Paare bilinearer Formen gab Frobenius[2]) eine Methode an, welche alle Irrationalitäten vermeidet. Indessen läßt sich das von ihm erhaltene rationale Kriterium für die Äquivalenz bilinearer Formen in einem beliebigen Körper auch durch bloße Modifikation der Weierstraßschen Methode herleiten.[3]) Hier soll eine noch einfachere rationale Methode entwickelt werden, die auf der Theorie der linearen Transformationen beruht.

56. Äquivalenz zweier Paare von Matrizen. In 30. hatten wir den Begriff der Äquivalenz zweier quadratischer Matrizen eingeführt. A und B waren äquivalent, wenn es zwei Matrizen P, Q gab, so daß $A = PBQ$. Dazu war, wie sich herausstellte, notwendig und hinreichend, daß die Rangzahlen für A und B gleich waren. — Entsprechend heißen nun zwei Paare von nn-Matrizen M, N und U, V mit Elementen aus K dann und nur dann in K äquivalent, wenn es nichtsinguläre $n$reihige Matrizen P und Q mit Elementen aus K gibt, so daß gleichzeitig

$$PMQ = U, \quad PNQ = V. \tag{1}$$

Unsere Aufgabe wird sein, die notwendigen und hinreichenden Kriterien für die Äquivalenz der Formenpaare festzustellen,

---

1) Berlin. Berichte 1868, p. 310; Werke II, 19.

2) Journal für Math. 86, 1879, pp. 146—208. — Betr. eines Berichtes über diese und verwandte Abhandlungen vergleiche man des Verfassers „History of Theory of Numbers", III, 1923, pp. 284—288.

3) Vgl. Dickson, Trans. Amer. Math. Soc., 10, 1909, pp. 347—360.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

ähnlich wie wir es auch im Falle einer einzelnen Form getan haben.

Wir behandeln zunächst den Fall, in dem N und V nichtsingulär sind. Für zwei solche äquivalente Paare ist $MN^{-1} = J$ ähnlich zu $UV^{-1} = W$; denn es ist

$$PJP^{-1} = PMQ \cdot Q^{-1}N^{-1}P^{-1} = UV^{-1} = W.$$

Daher haben die λ-Matrizen von J und W dieselben invarianten Faktoren. Andererseits hat aber nach 52. $J - \lambda E$ dieselben invarianten Faktoren wie

$$(J - \lambda E)N = (MN^{-1} - \lambda E)N = M - \lambda N.$$

Ebenso hat $W - \lambda E$ dieselben invarianten Faktoren wie $U - \lambda V$. Demnach haben auch $M - \lambda N$ und $U - \lambda V$ die gleichen invarianten Faktoren.

Umgekehrt folgt aus letzterem, daß die λ-Matrizen von J und W dieselben invarianten Faktoren haben, d. h. daß J und W in K ähnlich sind. Mit anderen Worten, es gibt eine nichtsinguläre Matrix P in K, so daß $P^{-1}JP = W$. Dann ist weiter

$$P(J - \lambda E)P^{-1} = W - \lambda E,$$
$$P(MN^{-1} - \lambda E)P^{-1} = UV^{-1} - \lambda E,$$
$$P(M - \lambda N)N^{-1}P^{-1} = (U - \lambda V)V^{-1},$$

also, wenn man Q für $N^{-1}P^{-1}V$ schreibt,

$$P(M - \lambda N)Q = U - \lambda V.$$

Durch Gleichsetzung der entsprechenden Potenzen von λ erhält man (1).

Satz 1: Zwei Paare quadratischer Matrizen M, N und U, V mit Elementen aus K, von denen N und V nichtsingulär sind, sind dann und nur dann in K äquivalent, wenn $M - \lambda N$ und $N - \lambda V$ dieselben invarianten Faktoren — oder, wenn wir wollen, dieselben Elementarteiler — haben.

Offenbar gilt dasselbe Kriterium auch für zwei Paare bilinearer Formen mit den Matrizen M, N und U, V.

57. Wir lassen nunmehr die Beschränkung, daß die Determinante $|N|$ von N nicht verschwindet, fallen, nehmen jedoch wenigstens an, daß $|M + xN|$ nicht identisch in x verschwindet, so daß wir also eine Zahl $v \neq 0$ aus K wählen können, für die $B = M + vN$ nichtsingulär ist. Sind jetzt die Paare M, N und

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

U, V in K äquivalent, so sind es auch die Paare M, B und $U, C = U + vV$ (wo C ebenfals nichtsingulär ist) und umgekehrt. Nach Satz 1 sind also die Paare M, N und U, V dann und nur dann in K äquivalent, wenn $M - \lambda B$ und $U - \lambda C$ dieselben invarianten Faktoren oder dieselben Elementarteiler haben. Hierzu ist aber notwendig und hinreichend, daß $\varrho M + \sigma N$ und $\varrho U + \sigma V$ dieselben Elementarteiler haben, wie wir mit folgendem Hilfssatz beweisen wollen.

Hilfssatz: Ist $A = pM + qN$, $B = uM + vN$ (*wo* $pv - qu \neq 0$), *also* $\mu A + \tau B = \varrho M + \sigma N$ *für*

$$\varrho = p\mu + u\tau, \quad \sigma = q\mu + v\tau, \tag{2}$$

so erhält man die Elementarteiler von $\mu A + \tau B$ *aus denen von* $\varrho M + \sigma N$ *durch die Transformation* (2).

Die Transformation (2) ersetzt jedes Element von $\varrho M + \sigma N$ durch das entsprechende Element von $\mu A + \tau B$, also auch jede $j$reihige Determinante von $\varrho M + \sigma N$ durch eine solche von $\mu A + \tau B$. Ist nun $(m\varrho + n\sigma)^e$ ein Teiler aller $j$reihigen Determinanten von $\varrho M + \sigma N$, und zwar von höchstmöglichem Exponenten, so wird dieser durch (2) in $(a\mu + b\tau)^e$ übergeführt, welches ein Teiler aller $j$reihigen Determinanten von $\mu A + \tau B$ mit wiederum höchstmöglichem Exponenten ist. Dann ergibt sich unser Satz aus der Definition der Elementarteiler von § 54.

Wir wenden diesen Satz für den Fall $p = u = 1$, $q = 0$, $v \neq 0$ an. Setzen wir dann noch $\mu = 1$, $\tau = -\lambda$, so haben wir die unserem Hilfssatz vorausgehenden Bezeichnungen. Damit sind wir im Besitze von

Satz 2: Es seien M, N, U, V *irgendwelche n-reihigen quadratischen Matrizen mit Elementen aus* K, *so daß keine der Determinanten* $|\varrho M + \sigma N|$ *und* $|\varrho U + \sigma V|$ *identisch in* ϱ *und* σ *verschwindet. Dann ist das Paar* M, N *dann und nur dann dem Paare* U, V *in* K *äquivalent, wenn* $\varrho M + \sigma N$ *und* $\varrho U + \sigma V$ *dieselben invarianten Faktoren (oder dieselben Elementarteiler) haben.*

Statt von den invarianten Faktoren von $\varrho M + \sigma N$ zu sprechen, sprechen wir kurz von den invarianten Faktoren des Paares bilinearer Formen mit den Matrizen M und N; ferner nennen wir den Fall, in dem $\varrho M + \sigma N$ in ϱ und σ nicht identisch verschwindet, kurz den ***nichtsingulären*** Fall. Dadurch erhält Satz 2 die knappere Form:

Satz 3: Im nichtsingulären Falle sind zwei Paare bilinearer Formen in $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ mit Koeffizienten aus K dann

Digitized by Google Original from UNIVERSITY OF MICHIGAN

und nur dann (gegenüber nichtsingulären Transformationen) in K äquivalent, wenn sie die gleichen invarianten Faktoren haben.

58. Kanonische Formen eines Paares bilinearer Formen. Ist N nichtsingulär, so ist das Paar M, N dem Paare $J = MN^{-1}$, $NN^{-1} = E$ äquivalent. Soll dies letztere einem anderen Paare, dessen zweites Element ebenfalls E ist, äquivalent sein, d. h. soll $PJQ = W$, $PEQ = E$ für nichtsinguläre P und Q sein, so muß $P = Q^{-1}$ sein. Das Paar J, E ist also dann und nur dann dem Paare W, E äquivalent, wenn $Q^{-1}JQ = W$, d. h. wenn J und W ähnlich sind.

Ist W sogar die Matrix der kanonischen Form der linearen Transformation mit der Matrix J, so nennen wir W, E das kanonische Paar von M, N.

Gehören alle Elemente von M und N einem Körper K an, so können wir W als die Matrix der kanonischen Form von Satz (1) des Kap. V (mit Koeffizienten aus K) voraussetzen. So ergibt sich

Satz 4: Jedes Paar bilinearer Formen in $x_1, \ldots, x_n, y_1, \ldots, y_n$ mit Koeffizienten aus K, dessen zweite Form nichtsingulär ist, läßt sich durch eine nichtsinguläre lineare Transformation der x und eine solche der y (jede mit Koeffizienten aus K) in ein einziges kanonisches Paar der Gestalt

$$f = \left(\sum_{i=1}^{a-1} x_i y_{i+1} + x_a \sum_{i=1}^{a} a_i y_i\right) + \left(\sum_{i=1}^{b-1} z_i w_{i+1} + z_b \sum_{1=i}^{b} b_i w_i\right) + \cdots$$

$$g = \sum_{i=1}^{a} x_i y_i + \sum_{i=1}^{b} z_i w_i + \cdots,$$

wo $a + b + \cdots = n$, überführen. Ist die Anzahl von $a, b, \ldots$ gleich k, so sind $1, \ldots, 1, I_{n-k+1}, \ldots,$

$$I_{n-1} = \lambda^b - \sum_{i=1}^{b} b_i \lambda^{i-1}, \quad I_n = \lambda^a - \sum_{i=1}^{a} a_i \lambda^{i-1}$$

die invarianten Faktoren von $f - \lambda g$.

Da $a_i, b_i, \ldots$ irgendwelche Zahlen aus K sind von der Eigenschaft, daß I_j in I_{j+1} enthalten ist (für $j < n$), so haben wir die

Folgerung: Es gibt ein Paar bilinearer Formen f, g in $n + n$ Variabeln mit Koeffizienten aus K von der Art, daß $f - \lambda g$ irgendwelche Polynome I_j mit Koeffizienten aus K, bei denen jedes I_j in I_{j+1} enthalten ist, als invariante Faktoren besitzt.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Wählen wir hingegen W als die Matrix der klassischen kanonischen Form des Satzes (13) von Kap. V, so erhalten wir anstatt Satz 4 den entsprechenden

Satz 5: Im Körper aller komplexer Zahlen läßt sich jedes Paar bilinearer Formen in $n+n$ Variabeln, dessen zweite Form nichtsingulär ist, auf das klassische kanonische Paar

$$\Phi = \left(R\sum_{i=1}^{r}\xi_i x_i + \sum_{i=2}^{r}\xi_i x_{i-1}\right) + \left(S\sum_{i=1}^{s}\eta_i y_i + \sum_{i=2}^{s}\eta_i y_{i-1}\right) + \cdots$$

$$\Psi = \sum_{i=1}^{r}\xi_i x_i + \sum_{i=1}^{s}\eta_i y_i + \cdots,$$

wo $r+s+\cdots = n$, zurückführen. Die Elementarteiler von $\Phi - \lambda\Psi$ sind $(\lambda - R)^r$, $(\lambda - S)^s$, ...

Folgerung: Schreibt man irgendwelche Potenzen

$$(\lambda - R)^r,\ (\lambda - S)^s, \ldots$$

vom Gesamtgrade n vor, so gibt es immer ein Paar bilinearer Formen Φ und Ψ, bei dem Ψ nichtsingulär ist, so daß $\Phi - \lambda\Psi$ diese Potenzen als Elementarteiler besitzt. —

Wir lassen nun wieder die Beschränkung $|N| \neq 0$ fallen, nehmen jedoch auch hier an, daß $|\varrho M + \sigma N|$ nicht identisch in ϱ und σ verschwindet. Es seien also u und v aus K so gewählt, daß $B = uM + vN$ nichtsingulär ist. Wählt man jetzt p und q aus K so, daß $pv - qu = 1$, und setzt $A = pM + qN$, so ist

$$M = vA - qB, \quad N = -uA + pB. \tag{3}$$

Das Paar A, B läßt sich auf rationale Weise auf ein Paar f, g nach Art des Satzes (4) zurückführen. Dieselben Transformationen reduzieren nun das Paar mit den Matrizen M und N auf das Paar $c = vf - qg$ und $d = -uf + pg$. Soll $\varrho c + \sigma d = \mu f + \tau g$, so muß

$$\mu = v\varrho - u\sigma, \quad \tau = -q\varrho + p\sigma, \tag{4}$$

welches im übrigen die Auflösung von (2) darstellt. Setzt man $\mu = 1, \tau = -\lambda$, so reduzieren sich die invarianten Faktoren von $\mu f + \tau g$ auf die von $f - \lambda g$. Machen wir umgekehrt die invarianten Faktoren von $f - \lambda g$ homogen in λ, μ und ersetzen dann λ durch $-\tau$, so erhalten wir die invarianten Faktoren von $\mu f + \tau g$. Schließlich ersetzt die Transformation (4) letztere durch die von $\varrho c + \sigma d$. Damit haben wir

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 6: Im nichtsingulären Fall läßt sich jedes Paar bilinearer Formen in den Variabeln $x_1, \ldots, x_n, y_1, \ldots, y_n$ mit Koeffizienten aus K vermittels einer nichtsingulären Transformation der x und einer solchen der y (jede mit Koeffizienten aus K) überführen in ein kanonisches Paar $c = vf - qg$ und $d = -uf + pg$, wo v, q, u, p Zahlen aus K mit der Bedingung $pv - qg = 1$ und f und g die Formen des Satzes 4 sind. Die invarianten Faktoren von $\varrho c + \sigma d$ erhält man durch Anwendung der Transformation (4) *aus denen von $\mu f + \tau g$, d. h. aus*

$$1, \ldots, 1, I_{n-k+1}, \ldots,$$

$$I_{n-1} = \tau^b - \sum_{j=0}^{b-1} b_{j+1} \tau^j (-\mu)^{b-j},$$

$$I_n = \tau^a - \sum_{j=0}^{a-1} a_{j+1} \tau^j (-\mu)^{a-j}. \quad —$$

Ist $(\lambda - R)^r$ ein Elementarteiler von $A - \lambda B$, so ist $(\tau + \mu R)^r$ ein solcher von $\mu A + \tau B$, und umgekehrt. Nach dem Hilfssatz aus 57. ersetzt die Inverse (4) der Transformation (2) einen Elementarteiler $(\tau + \mu R)^r$ von $\mu A + \tau B$ durch einen Elementarteiler $(m_1 \varrho + n_1 \sigma)^r$ von $\varrho M + \sigma N$. Da jedoch nur das Verhältnis von m_1 und n_1 wesentlich ist, so können wir $m_1 u + n_1 v = 1$ setzen. Ist dann $R = m_1 p + n_1 q$, so haben wir $m_1 \varrho + n_1 \sigma = \tau + \mu R$. Nach Satz 5 können wir das Paar bilinearer Formen mit den Matrizen A und B auf das kanonische Paar Φ und Ψ reduzieren. Dann reduziert sich dasjenige mit den Matrizen (3) auf das Paar $\alpha = v\Phi - q\Psi$ und $\beta = -u\Phi + p\Psi$, deren explizite Ausdrücke sich in Satz 7 finden. Denn aus $pv - qu = 1$, $m_1 u + n_1 v = 1$, $m_1 p + n_1 q = R$ folgt $m_1 = vR - q$, $n_1 = p - uR$. — Ersetzen wir R durch S und den Index 1 durch 2, so haben wir entsprechend $m_2 = vS - q$, $n_2 = p - uS$.

Satz 7: Im nichtsingulären Fall kann jedes Paar bilinearer Formen in $n + n$ Variabeln auf das klassische kanonische Paar

$$\alpha = \left(m_1 \sum_{i=1}^{r} \xi_i x_i + v \sum_{i=2}^{r} \xi_i x_{i-1}\right) + \left(m_2 \sum_{i=1}^{s} \eta_i y_i + v \sum_{i=2}^{s} \eta_i y_{i-1}\right) + \cdots,$$

$$\beta = \left(n_1 \sum_{i=1}^{r} \xi_i x_i - u \sum_{i=2}^{r} \xi_i x_{i-1}\right) + \left(n_2 \sum_{i=1}^{s} \eta_i y_i - u \sum_{i=2}^{s} \eta_i y_{i-1}\right) + \cdots$$

reduziert werden.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Die Elementarteiler von $\varrho\alpha + \sigma\beta$ *sind*

$$(m_1\varrho + n_1\sigma)^r, \quad (m_2\varrho + n_2\sigma)^s, \ldots$$

Folgerung: Es gibt immer ein Paar bilinearer Formen α und β in $n + n$ Variabeln von der Art, daß $\varrho\alpha + \sigma\beta$ eine nicht identisch in ϱ, σ verschwindende Determinante und irgendwelche vorgeschriebenen Elementarteiler vom Gesamtgrade n besitzt.

Übungen: 1. Zwei quadratische Formen mit den Matrizen A und B haben als Invarianten vom Gewicht 2 die Koeffizienten der verschiedenen Potenzen von λ in der Determinante von $A - \lambda B$.

2. Gib unter Benutzung von Satz 5 die drei Typen von kanonischen Paaren bilinearer ternärer Formen an.

59. Büschel bilinearer Formen. Anstatt eines Paares bilinearer Formen μ und ν mit Koeffizienten aus K betrachten wir das ganze Büschel $[\mu, \nu]$, das aus allen Formen $\varrho\mu + \sigma\nu$ besteht, wo ϱ und σ zu K gehören. Dieses Büschel ist offenbar mit dem Büschel $[\alpha, \beta]$ identisch, wenn

$$\alpha = p\mu + q\nu, \quad \beta = u\mu + v\nu, \quad pv - qu \neq 0. \tag{5}$$

Das Büschel heißt nichtsingulär, wenn die Determinante von $\varrho\mu + \sigma\nu$ nicht identisch in ϱ, σ verschwindet.

Ein zweites solches Büschel $[\mu_1, \nu_1]$ ist dann und nur dann in K dem Büschel $[\mu, \nu]$ äquivalent, wenn das Paar μ_1, ν_1 einem Paar (5) des Büschels $[\mu, \nu]$ äquivalent ist.

Mit Rücksicht auf unseren Hilfssatz und auf Satz 2 haben wir

Satz 8: Sind M, N, M_1, N_1 *die Matrizen der bilinearen Formen* μ, ν, μ_1, ν_1 *mit Koeffizienten aus* K, *so sind die nichtsingulären Büschel* $[\mu, \nu]$ *und* $[\mu_1, \nu_1]$ *dann und nur dann in* K *äquivalent, wenn sich alle invarianten Faktoren (oder Elementarteiler) von* $\varrho_1 M_1 + \sigma_1 N_1$ *aus denen von* $\varrho M + \sigma N$ *durch dieselbe nichtsinguläre lineare Transformation aus* K, *die* ϱ *und* σ *linear durch* ϱ_1 *und* σ_1 *ausdrückt, herleiten lassen.*

60. Die $n$ten Wurzeln einer Matrix. Wir benötigen den

Hilfssatz: Sind $a, b, c, \ldots$ *voneinander verschieden und nicht gleich Null, bezeichnet man ferner mit* $\psi(x)$ *den Ausdruck*

$$\psi(x) = (x - a)^r (x - b)^s (x - c)^t \ldots,$$

so existiert ein Polynom $\chi(x)$ *von der Art, daß* $[\chi(x)]^n - x$ *durch* $\psi(x)$ *teilbar ist.*

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ist z. B. $n = 2$ und $\psi = (x-a)^2$, so ist

$$\chi = \frac{1}{2} a^{-\frac{1}{2}} (x+a), \quad \chi^2 - x = \frac{1}{4} a^{-1} (x-a)^2.$$

Zum Beweise entwickle man nach dem binomischen Lehrsatz $\sqrt[n]{x}$ nach steigenden Potenzen von $x-a$:

$$\sqrt[n]{x} = \sqrt[n]{a} \cdot \sqrt[n]{1 + \frac{(x-a)}{a}}$$

$$= \sqrt[n]{a} \left[1 + \frac{x-a}{na} + \frac{(1-n)(x-a)^2}{2n^2a^2} + \cdots\right]$$

und bezeichne die Summe der r ersten Glieder mit $F(x)$, so daß $\sqrt[n]{x} - F(x)$ gliedweise durch $(x-a)^r$ teilbar ist. Ebenso bezeichne man mit $G(x)$ die Summe der s ersten Glieder der Entwicklung von $\sqrt[n]{x}$ in der Umgebung von $x-b$, so daß $\sqrt[n]{x} - G(x)$ durch $(x-b)^s$ teilbar ist; usw.

Durch Zerlegung in Partialbrüche erhält man

$$\frac{F(x)}{\psi(x)} = \frac{A_0}{(x-a)^r} + \cdots + \frac{A_{r-1}}{x-a} + R(x)$$

$$\equiv \frac{A(x)}{(x-a)^r} + \frac{(x-a)^r P(x)}{\psi(x)},$$

wo die A_i Konstante sind und $R(x)$ der Quotient eines Polynoms $P(x)$ und $\frac{\psi(x)}{(x-a)^r}$ ist. Wie man durch Multiplizieren mit $\psi(x)$ sieht, haben die r ersten Glieder des nach Potenzen von $x-a$ entwickelten Ausdrucks $\frac{\psi(x) A(x)}{(x-a)^r}$ die Summe $F(x)$ und sind daher mit den r ersten Gliedern der Entwicklung von $\sqrt[n]{x}$ identisch. D. h. die Differenz zwischen jenem Bruch und $\sqrt[n]{x}$ enthält den Faktor $(x-a)^r$.

Nunmehr bestimme man $B(x)$ aus $G(x)$ ebenso wie eben $A(x)$ aus $F(x)$. Dann ist die Differenz zwischen $\sqrt[n]{x}$ und dem zweiten Gliede der rechten Seite von

$$\chi(x) = \frac{\psi(x) A(x)}{(x-a)^r} + \frac{\psi(x) B(x)}{(x-b)^s} + \cdots$$

durch $(x-b)^s$ teilbar. Die anderen Glieder sind wegen des Faktors $\psi(x)$ von selbst durch $(x-b)^s$ teilbar. Es ist also $\chi - \sqrt[n]{x}$ durch $(x-b)^s$ und ebenso durch $(x-a)^r, \ldots$, demnach auch durch ihr Produkt $\psi(x)$ teilbar. —

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 9: Ist X eine nichtsinguläre quadratische Matrix, so existiert ein Polynom $\chi(\lambda)$ von der Art, daß die $n$te Potenz der Matrix $\chi(X)$ gleich X ist. $\chi(X)$ heißt daher eine $n$te Wurzel von X.

In 25. zeigten wir, daß, wenn $\varphi(\lambda)$ die charakteristische Determinante von X ist, $\varphi(X) = 0$. Da X nichtsingulär ist, so verschwindet das konstante Glied von $\varphi(\lambda)$ nicht. $\varphi(\lambda)$ erfüllt daher daher die Bedingungen des $\psi(\lambda)$ unseres Hilfssatzes, und es gibt demnach Polynome $\chi(\lambda)$ und $q(\lambda)$, für die

$$[\chi(\lambda)]^n - \lambda \equiv \varphi(\lambda) q(\lambda)$$

identisch in λ. Da auf beiden Seiten die Koeffizienten gleicher Potenzen von λ gleich sind und da auch für Matrizen die Gleichung $X^i X^j = X^{i+j}$ gilt, so kann man an Stelle von λ auch X in die obige Gleichung einsetzen und erhält so

$$[\chi(X)]^n - X = \varphi(X) q(X) = 0.$$

61. Äquivalenz von Paaren quadratischer sowie symmetrischer bilinearer Formen. Die Theorie der Äquivalenz von Paaren bilinearer Formen läßt sich, wie wir in 56. sahen, in jedem Bereich auf rationale Weise entwickeln. Dasselbe gilt jedoch nicht mehr für Paare quadratischer Formen, zu deren Untersuchung wir vielmehr Satz 9, d. h. die Einführung von Irrationalitäten notwendig haben. Daß sich die Irrationalitäten auch bei keiner anderen Methode umgehen lassen, ersieht man aus folgendem Beispiel: Die reellen quadratischen Formen $x^2 - 2y^2$ und $x^2 - 3y^2$ gehen durch die Transformation $x = z$, $y = \sqrt{-1} \cdot w$ in $z^2 + 2w^2$ bzw. $z^2 + 3w^2$ über. Jedoch ist diese Überführung mittels einer reellen Transformation nicht möglich, da die ersten Formen reelle Faktoren haben, die letzteren nicht. Wir müssen demnach bei unserer Untersuchung der Äquivalenz den Körper aller komplexen Zahlen zugrunde legen.

Wir gehen aus von vier bilinearen symmetrischen Formen α, β, γ, δ mit den Matrizen A, B, C, D. Nach Kap. III, Satz 7 ist das Paar α, β gegenüber einer nichtsingulären Transformation der x und y mit der Matrix M dann und nur dann dem Paar γ, δ äquivalent, wenn

$$C = M'AM, \quad D = M'BM, \quad |M| \neq 0. \tag{6}$$

Lassen wir y_i mit $x_i (i = 1, \ldots, n)$ zusammenfallen, so entstehen zwei Paare quadratischer Formen. Zu ihrer Äquivalenz ist ebenfalls notwendig und hinreichend, daß ihre Matrizen die Beziehung (6) erfüllen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Satz 10: Wenn die n-reihigen quadratischen Matrizen A, B, C, D symmetrisch sind und das Paar A, B dem Paar C, D äquivalent ist, d. h. wenn es nichtsinguläre n-reihige quadratische Matrizen P und Q gibt, so daß

$$C = PAQ, \quad D = PBQ, \tag{7}$$

so gibt es eine nichtsinguläre n-reihige quadratische Matrix M, für welche die Beziehungen (6) *gelten.*

Nach Voraussetzung ist

$$C = C' = Q'A'P' = Q'AP'. \tag{8}$$

Durch Gleichsetzen mit $C = PAQ$ erhält man

$$(Q')^{-1}PA = AP'Q^{-1}.$$

Führt man zur Abkürzung

$$X = (Q')^{-1}P \tag{9}$$

ein, wo also X nichtsingulär ist, so ergibt sich

$$XA = AX', \quad X^2A = XAX' = A(X')^2$$

und allgemein durch Induktion

$$X^kA = A(X')^k. \tag{10}$$

Bezeichnet $\chi(x) = \sum c_k x^k$ ein beliebiges Polynom in x, so erhält man aus (10) durch Multiplikation mit c_k $(k = 0, 1, \ldots)$ und Addition

$$\chi(X) \cdot A = A \cdot \chi(X'). \tag{11}$$

Wir wählen nun, was nach Satz 9 möglich ist, die komplexen Koeffizienten c_k so, daß das Quadrat der Matrix $V = \chi(X)$ gleich X wird. Mit X ist auch $V^2 = X$, also auch V selbst nichtsingulär. Dann erhält (11) die Form

$$A = V^{-1}AV'$$

und (7_1) geht über in

$$C = PV^{-1}AV'Q.$$

Wegen (9) und $V^2 = X$ ist $Q'V = PV^{-1}$. Setzt man noch $M = V'Q$, so wird in der Tat $C = M'AM$, wie in (6) behauptet wurde.

Da mit X und V auch M nur von P und Q, jedoch nicht von A oder C abhängt, so ergibt sich ähnlich die zweite Gleichung (6) aus der zweiten Gleichung (7). —

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Aus Satz 10 und 3 folgt offenbar

Satz 11: Damit im nichtsingulären Fall zwei Paare symmetrischer bilinearer Formen gegenüber einer nichtsingulären linearen Transformation der x und der kogredienten Transformation der y äquivalent sind, ist notwendig und hinreichend, daß sie dieselben invarianten Faktoren haben.

Hieraus und aus Folgerung 1 des § 33 ergibt sich wiederum

Satz 12: Im nichtsingulären Fall sind zwei Paare quadratischer Formen dann und nur dann gegenüber einer nichtsingulären Transformation äquivalent, wenn sie dieselben invarianten Faktoren haben.

Greifen wir schließlich noch den Fall heraus, wo die zweite quadratische Form jedes Paares gleich $\sum x_i^2$ ist, also die Einheitsmatrix E besitzt, so folgt aus Satz 12 die

Folgerung: Zwei quadratische Formen A und C sind dann und nur dann gegenüber einer orthogonalen Transformation äquivalent, wenn ihre λ-Matrizen $A - \lambda E$ und $C - \lambda E$ dieselben invarianten Faktoren haben. —

Die Bedingung dafür, daß zwei Paare reeller quadratischer Formen gegenüber reellen Transformationen äquivalent sind, ist zu kompliziert, um hier Platz finden zu können.[1])

Übungen: 1. Jede binäre quadratische nichtsinguläre Form kann durch eine reelle oder imaginäre orthogonale Transformation in einer der Formen

$$ax^2 + by^2 (a \neq b); \quad ax^2 + ay^2; \quad 2ax^2 + 2aixy,$$

übergeführt werden, je nachdem sie die invarianten Faktoren 1, $(\lambda - a)(\lambda - b)$; $\lambda - a$, $\lambda - a$ oder 1, $(\lambda - a)^2$ hat.

2. Im nichtsingulären Fall lassen sich zwei quadratische Formen f und h dann und nur dann in Formen, welche nur die Quadrate der Variabeln enthalten, überführen, wenn ihre Elementarteiler alle vom ersten Grade sind. Nach 37. ist daher letzteres sicher der Fall, wenn f eine reelle quadratische und h eine positive nichtsinguläre Form ist.

62. Paare, in denen alternierende Formen vorkommen. Eine bilineare Form mit der Matrix A heißt alternierend, wenn $A' = -A$. (Vgl. Beispiel 4 in 38).

Satz 13: Satz 10 gilt auch dann noch, wenn

$$A' = -A, \quad C' = -C, \quad B' = \pm B, \quad D' = \pm D.$$

1) Vgl. Muth, Journal für Math. 128, 1905, pp. 302—321. — Über Paare binärer quadratischer Formen in einem beliebigen Bereich vergleiche man Dickson, Amer. Journ. Math. 31, 1909, pp. 103—108.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Denn aus (7_1) folgt in diesem Falle

$$C = -C' = -Q'A'P' = +Q'AP',$$

so daß (8) auch hier bestehen bleibt. Der übrige Beweis von Satz 10 bleibt unverändert.

Aus Satz 13 und 3 folgt entsprechend zu Satz 11:

Satz 14: Damit im nichtsingulären Falle zwei Paare von Formen α, β und γ, δ, von denen α und γ alternierende bilineare Formen, β und δ hingegen entweder alternierende oder symmetrische bilineare Formen sind, gegenüber einer nichtsingulären Transformation der x und der kogredienten Transformation der y äquivalent sind, ist notwendig und hinreichend, daß sie dieselben invarianten Faktoren haben.

Ist α eine symmetrische, β eine alternierende bilineare Form, so treten alle Elementarteiler von $\varrho\alpha + \sigma\beta$, welche die Gestalt ϱ^{2k} oder σ^{2k+1} haben, paarweise auf.[1])

63. Das Weierstraßsche kanonische Paar quadratischer Formen. Wir werden zunächst ein Paar (12) quadratischer Formen mit einem einzigen von 1 verschiedenen invarianten Faktor I aufstellen, wo I ein vorgeschriebenes Polynom ist. Es sei

$$I = \prod_{j=1}^{k} (\lambda - \lambda_j)^{e_j}.$$

Ist jedes c_j und d_j von Null verschieden, so hat das Paar

$$(12)\qquad \begin{aligned} \gamma &= \sum_{j=1}^{k} \left[\lambda_j c_j \sum_{i=1}^{e_j} x_{ij} x_{e_j - i + 1, j} + d_j \sum_{i=1}^{e_j - 1} x_{ij} x_{e_j - i, j} \right], \\ \delta &= \sum_{j=1}^{k} c_j \sum_{i=1}^{e_j} x_{ij} x_{e_j - i + 1, j} \end{aligned}$$

in der Tat die invarianten Faktoren $1, \ldots, 1, I$. Zum Beweise schreibe man die Matrix von $\gamma - \lambda\delta$ in der abgekürzten Bezeichnung

---

1) Kronecker, Monatsber. Akad. Berlin 1874, p. 397; Werke I, p. 423. — Betr. des Beweises vgl. Frobenius in der Encyclop. Sciences Math., t. I, vol. II, pp. 463—69, sowie Muth, Elementarteiler, 1899, pp. 135—142; pp. 231—232.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$$\begin{pmatrix} M_1 & 0 & 0 \dots 0 & 0 \\ 0 & M_2 & 0 \dots 0 & 0 \\ \cdot & \cdot & \cdot \cdot \cdot & \cdot \\ 0 & 0 & 0 \dots 0 & M_k \end{pmatrix},$$

wo 0 eine Nullmatrix und M_j die $e_j$reihige quadratische Matrix derjenigen Glieder von $\gamma - \lambda\delta$ ist, in denen j einen festen Wert hat, d. h.

$$M_j = \begin{pmatrix} 0 & 0 & 0 \dots 0 & 0 & c_j(\lambda_j - \lambda) \\ 0 & 0 & 0 \dots d_j & c_j(\lambda_j - \lambda) & 0 \\ \cdot & \cdot & \cdot \cdot \cdot & \cdot & \cdot \\ d_j & c_j(\lambda_j - \lambda) & 0 \dots 0 & 0 & 0 \\ c_j(\lambda_j - \lambda) & 0 & 0 \dots 0 & 0 & 0 \end{pmatrix},$$

wo also die Elemente der Nebendiagonale alle gleich $c_j(\lambda_j - \lambda)$, die unmittelbar links von ihnen stehenden alle gleich d_j und alle übrigen Elemente gleich Null sind. Abgesehen von konstanten Faktoren ist also die Determinante von M_j gleich $(\lambda - \lambda_j)^{e_j}$ und der Minor des letzten Elementes der letzten Zeile ist konstant gleich $d_j^{e_j - 1} \neq 0$. Nunmehr ergibt sich wie im ersten Teile von 53., daß 1, 1, ..., 1, I die invarianten Faktoren von $\gamma - \lambda\delta$ sind.

Jetzt seien $I_1, \dots, I_t$ irgendwelche vorgeschriebenen Polynome $\lambda^{m_1} + \cdots, \cdots$ von der Art, daß I_s für jedes s in I_{s+1} enthalten ist. Wir stellten soeben ein Paar γ_s, δ_s von quadratischen Formen mit den invarianten Faktoren 1, ..., 1, I_s auf. Wenn nun keine Variable von γ_s bzw. δ_s in γ_i bzw. δ_i $(i \neq s)$ vorkommt, so sind, wie in 43. bewiesen wurde, $I_1, \dots, I_t$ die einzigen von 1 verschiedenen invarianten Faktoren von $\sum\gamma_s$, $\sum\delta_s$.

Die höchsten Potenzen der unter allen invarianten Faktoren vorkommenden linearen Funktionen haben also die Form $(\lambda - \lambda_j)^{e_j}$ $(j = 1, \dots, m)$. Damit haben wir

Satz 15: Es gibt immer ein Paar quadratischer Formen, das irgendwelche vorgeschriebenen Elementarteiler

$$(\lambda - \lambda_1)^{e_1}, \dots, (\lambda - \lambda_m)^{e_m} \quad \textbf{besitzt.}$$

Die Zahl der Variabeln sei z. B. drei. Dann haben wir die **Fälle**:

1. $e_1 = e_2 = e_3 = 1$. Man setze $c_1 = c_2 = 1$, $c_3 = -1$ und schreibe x_j anstatt x_{1j}. Dann ist

$$\gamma = \lambda_1 x_1^2 + \lambda_2 x_2^2 - \lambda_3 x_3^2, \quad \delta = x_1^2 + x_2^2 - x_3^2.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Sind alle λ voneinander verschieden, so haben die Kegelschnitte $\gamma = 0$ und $\delta = 0$ vier verschiedene Schnittpunkte, die sich aus

$$x_1^2 : x_2^2 : x_3^2 = \lambda_2 - \lambda_3 : \lambda_3 - \lambda_1 : \lambda_2 - \lambda_1$$

ergeben. — Ist jedoch $\lambda_1 \neq \lambda_2 = \lambda_3$, so existieren nur zwei Schnittpunkte $x_1 : x_2 : x_3 = 0 : 1 : \pm 1$, und die Kegelschnitte berühren sich in ihnen. — Ist endlich $\lambda_1 = \lambda_2 = \lambda_3 \neq 0$, so fallen die Kegelschnitte zusammen.

2. $e_1 = 2$, $e_2 = 1$. Man setze $c_1 = c_2 = d_1 = 1$ und schreibe x_1, x_2, x_3 anstatt x_{11}, x_{21}, x_{12}. Dann ist

$$\gamma = 2\lambda_1 x_1 x_2 + x_1^2 + \lambda_2 x_3^2, \quad \delta = 2x_1 x_2 + x_3^2.$$

Für $\lambda_1 = \lambda_2$ ist $x_1 = x_3 = 0$ der einzige Schnittpunkt, die Kegelschnitte berühren sich in ihm vierpunktig. — Für $\lambda_1 \neq \lambda_2$ gibt es zwei weitere Schnittpunkte, für welche

$$x_1 = 2(\lambda_2 - \lambda_1) x_2, \quad x_3^2 = -4(\lambda_2 - \lambda_1) x_2^2,$$

und die Kegelschnitte berühren sich in $x_1 = x_3 = 0$ nur zweipunktig.

3. $e_1 = 3$. Man setze $c_1 = d_1 = 1$ und unterdrücke bei den x die zweiten Indizes. Dann ist

$$\gamma = \lambda_1(2x_1 x_3 + x_2^2) + 2x_1 x_2, \quad \delta = 2x_1 x_3 + x_2^2.$$

Die Kegelschnitte berühren sich in $x_1 = x_2 = 0$ dreipunktig und schneiden sich in $x_2 = x_3 = 0$.

Übungen: 1. Man stelle die kanonischen Formen von Paaren quaternärer quadratischer Formen auf.

2. Sind A und N irgend zwei $n$reihige quadratische Matrizen, so existiert eine $n$reihige nichtsinguläre Matrix X, für die $X'AX = N$, dann und nur dann, wenn das Paar A, A' dem Paare N, N' äquivalent ist. — Anleitung: Zu ihrer Äquivalenz ist notwendig, daß es Matrizen P, Q gibt, für die $PAQ = N$, $PA'Q = N'$. Auf die Formen $A - A', A + A', N - N', N + N'$ wende man dann Satz 13 an.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

SIEBENTES KAPITEL.

PAARE VON BILINEAREN UND QUADRATISCHEN FORMEN IM SINGULÄREN FALLE.

Den Gegenstand dieses Kapitels bildet die Theorie der Äquivalenz von Paaren bilinearer und quadratischer Formen im singulären Falle. Der erste, der auf dieses Problem stieß, war Kronecker.[1]) Im Gegensatz zu seiner Methode, die von der Weierstraßschen irrationalen kanonischen Form ausgeht, ist die hier angewandte Methode, welche die rationale kanonische Form benutzt, zum ersten Male rein rational.[2])

64. Paare von bilinearen Formen im singulären Falle. φ und ψ seien bilineare Formen in denselben Variabeln $x_1, \ldots, x_r$, $y_1, \ldots, y_s$ mit Koeffizienten aus K, die sich nicht auf Formen mit weniger als r Variabeln x_i oder s Variabeln y_i zurückführen lassen. Wir setzen voraus, daß die Determinante von $f = u\varphi + v\psi$ identisch in u und v verschwindet (was im Falle $r \neq s$ von selbst erfüllt ist). Ist ferner $r \neq s$, so können wir — nötigenfalls nach Vertauschung von x und y — annehmen, daß $r > s$.

Man bezeichne die partiellen Ableitungen von f, φ, ψ nach x_i mit f_i, φ_i, ψ_i. Dann sind die $r \geqq s$ linearen Funktionen $f_1, \ldots, f_r$ von $y_1, \ldots, y_s$ voneinander abhängig. Es sei $\sum A_i f_i \equiv 0$ (in $u, v, y_1, \ldots, y_s$) eine zwischen den f_i bestehende Beziehung, in der nicht alle A_i identisch verschwindende, homogene Polynome von gleichem Grade in u, v mit Koeffizienten aus K sind.

---

1) Sitzungsberichte der Akademie der Wissenschaften, Berlin 1890, pp. 1225—37. — Sein kurzer Bericht wurde von Muth in seinem Buche über „Elementarteiler", 1899, pp. 93—133 ausgearbeitet. Einige unbedeutende Druckfehler dieses Buches sind in den Bericht in der „Encyclopédie des Sciences Mathémathiques", tome I, vol. II, 1911, pp. 412—425 übergegangen.

2) Dickson, Singular Case of bilinear, quadrat. or hermit. Forms, Trans. Amer. Math. Soc. XXIX, Nr. 2, 1927, pp. 239—253.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Nun gilt der

Hilfssatz 1: Unterwerfen wir in f die x und y je einer linearen nichtsingulären Transformation mit von u und v unabhängigen Koeffizienten, so bleibt der Grad der A_i in u, v ungeändert.

Transformiert man nur die y, so ist der Satz offenbar richtig. Werden jetzt auch die x, und zwar in die neuen Variabeln X transformiert, so möge f in g übergehen. Ist also

$$X_j = \sum_{i=1}^{r} a_{ji} x_i,$$

so ist

$$f_i = \sum_{j=1}^{r} \frac{\partial g}{\partial X_j} \cdot \frac{\partial X_j}{\partial x_i} = \sum_{j=1}^{r} a_{ji} g_i.$$

Da nun $\sum A_i f_i \equiv 0$, so ist auch $\sum B_j g_j \equiv 0$, wo $B_j = \sum_i a_{ji} A_i$ vom selben Grade ist wie A_i.

Von allen Beziehungen der Art $\sum A_i f_i \equiv 0$ greifen wir nun eine heraus:

$$(1) \qquad \sum_{i=1}^{r} A_i f_i \equiv \sum_{\alpha=0}^{m} (-1)^\alpha C_\alpha u^\alpha v^{m-\alpha} \equiv 0,$$

nämlich die, in welcher die A_i nicht alle identisch verschwinden und von möglichst niedrigem Grade sind. Dabei sind die Koeffizienten von A_i herausgenommen und mit f_i vereinigt worden zu C_α:

$$(2) \qquad C_\alpha = \sum_{i=1}^{r} c_{\alpha i} f_i \qquad (\alpha = 0, 1, \ldots, m).$$

Nach Hilfssatz 1 ist m eine numerische Invariante des Paares φ, ψ gegenüber allen nichtsingulären Transformationen der x bzw. y.

Wie wir sahen, erfüllen die f_i eine lineare Beziehung, in welcher jedoch die Koeffizienten Polynome sind. Wir werden nunmehr zeigen, daß in der Tat keine Beziehung möglich ist, in der die Koeffizienten Zahlen sind. Denn wenn $\sum t_i f_i \equiv 0$ wäre, wo die t_i zu K gehören und nicht alle verschwinden, so müßte, da $f_i = u\varphi_i + v\psi_i$, auch

$$\sum t_i \varphi_i \equiv 0, \quad \sum t_i \psi_i \equiv 0.$$

Es sei nun t_e einer der nichtverschwindenden Koeffizienten. Dann geht $\varphi = \sum x_i \varphi_i$ durch die nichtsinguläre Transformation

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$$x_\varrho = t_\varrho X_\varrho, \quad x_j = X_j + t_j X_\varrho \qquad (j = 1, \ldots, r; j \neq \varrho)$$

in

$$\sum_{j \neq \varrho} X_j \varphi_j + X_\varrho \sum_{i=1}^{r} t_i \varphi_i$$

über. In dieser Form kommt jedoch X_ϱ nicht mehr vor, da die zweite Summe verschwindet. Ebenso kommt X_ϱ in ψ nicht vor. Das widerspricht aber unserer Voraussetzung, nach der die Zahl der Variabeln nicht heruntergedrückt werden kann. Wir haben demnach

Hilfssatz 2: In K sind die f_i linear unabhängig.

Folgerung: Die Invariante m ist > 0.

Denn für $m = 0$ geht (1) in $C_0 = 0$ über, und aus (2) folgt, daß jedes $c_{\alpha i} = 0$, gegen die Voraussetzung. —

Hilfssatz 3: $C_0, \ldots, C_m$ sind in K linear unabhängig.

Denn angenommen, es gebe Zahlen $a_0, \ldots, a_m$ aus K, die nicht alle verschwinden und für die

$$\sum_{\alpha=0}^{m} a_\alpha C_\alpha \equiv 0. \tag{3}$$

Die in (1) auftretenden Summen bezeichne man mit Q bzw. R. Setzt man dann

$$P = \sum_{\alpha=0}^{m} (-1)^\alpha a_\alpha u^{m-\alpha} v^\alpha, \tag{4}$$

so ist jedes PA_i ein Polynom in u und v vom Grade $2m$; den Koeffizienten von $u^m v^m$ bezeichne man mit k_i. Da man nun die Glieder $\sum k_i u^m v^m f_i$ von PQ aus den Gliedern $\sum a_\alpha C_\alpha u^m v^m$ von PR erhält, wenn man C_α durch seinen Wert (2) ersetzt, so folgt aus (3), daß $\sum k_i f_i \equiv 0$, und aus Hilfssatz 2, daß jedes $k_i = 0$. Daher nimmt $PQ \equiv 0$ die Form an

$$v^{m+1} \sum f_i g_i + u^{m+1} \sum f_i h_i \equiv 0 \qquad (i = 1, \ldots, r), \tag{5}$$

in der g_i und h_i Polynome vom Grade $m - 1$ in u, v sind. Sie können nicht alle identisch verschwinden, sonst wäre dasselbe für jedes PA_i, also auch für jedes A_i der Fall. Ersetzt man f_i durch seinen Wert $u\varphi_i + v\psi_i$, so sieht man, daß der erste Teil in (5) vom Grade $\leqq m$, der zweite hingegen vom Grade $> m$ in u ist. Daher verschwinden beide Teile identisch, und der eine von ihnen liefert eine lineare Beziehung zwischen $f_1, \ldots, f_r$, deren Koeffizienten nicht alle identisch verschwinden und in u, v den Grad

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$m - 1$ haben. Das widerspricht aber unserer Annahme, nach der m der Minimalgrad sein soll. —

Nach den Hilfssätzen 2 und 3 hat nun die Matrix der Koeffizienten $c_{\alpha i}$ in (2) mindestens eine nichtverschwindende Determinante von der Ordnung $m + 1$. Wir können daher Zeilen, deren Elemente Zahlen aus K sind, hinzufügen, so daß eine quadratische Matrix

$$(c_{\alpha\beta}) \qquad (\alpha = 0, 1 \ldots, r-1;\ \beta = 1, \ldots, r)$$

von nichtverschwindender Determinante entsteht. Durch die lineare nichtsinguläre Transformation

$$x_\beta = \sum_{\alpha=0}^{r-1} c_{\alpha\beta} X_\alpha \qquad (\beta = 1, \ldots, r), \tag{6}$$

deren Koeffizienten von u, v unabhängig sind, mögen nun f, φ, ψ in F, Φ, Ψ übergehen. Bezeichnet man noch die partiellen Ableitungen der letzteren nach X_i mit F_i, Φ_i, Ψ_i, so wird wegen (2)

$$F_\alpha = \sum_{\beta=1}^{r} \frac{\partial f}{\partial x_\beta} \cdot \frac{\partial x_\beta}{\partial X_\alpha} = \sum_{\beta=1}^{r} c_{\alpha\beta} f_\beta = C_\alpha, \tag{7}$$

mithin wegen (1) $\quad \sum (-1)^\alpha F_\alpha u^\alpha v^{m-\alpha} \equiv 0.$

Ersetzt man F_α durch $u\Phi_\alpha + v\Psi_\alpha$ und setzt die Koeffizienten von $v^{m+1}, uv^m, \ldots, u^m v, u^{m+1}$ gleich Null, so erhält man

$$\Psi_0 \equiv 0,\ \Psi_1 \equiv \Phi_0,\ \Psi_2 \equiv \Phi_1, \ldots,\ \Psi_m \equiv \Phi_{m-1}, \Phi_m \equiv 0, \tag{8}$$

d. h. es ist

$$F_0 \equiv u\Psi_1,\ F_1 \equiv u\Psi_2 + v\Psi_1, \ldots, F_{m-1} \equiv u\Psi_m + v\Psi_{m-1},$$
$$F_m \equiv v\Psi_m.$$

Multipliziert man die ersten k Gleichungen nacheinander mit $v^{k-1}, -uv^{k-2}, \ldots, (-u)^{k-2}v, (-u)^{k-1}$ und addiert, so erhält man

$$-(-u)^k \Psi_k \equiv \sum_{i=0}^{k-1} F_i (-u)^i v^{k-i-1} \qquad (k = 1, \ldots, m). \tag{9}$$

Wenn also die Ψ_i eine lineare Beziehung erfüllen, deren Koeffizienten zu K gehören und nicht alle verschwinden, so multipliziere man diese Beziehung mit u^m und forme nach (9) um. Man erhält dadurch eine lineare Gleichung zwischen $F_0, \ldots, F_{m-1}$, deren Koeffizienten nicht identisch verschwindende Polynome vom Grade $m - 1$ in u, v sind, und durch Einsetzen von (7) unter

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Anwendung von (2) eine ähnliche Gleichung zwischen den f_i, was aber der Definition von m widerspricht. Da demnach $\Psi_1, \ldots, \Psi_m$ in K linear unabhängig sind, so kann man noch andere lineare Funktionen $Y_{m+1}, \ldots, Y_s$ von $y_1, \ldots, y_s$ mit Koeffizienten aus K hinzunehmen, von der Art, daß noch immer die Ψ und Y in K unabhängig sind. Durch die Transformation

$$(10) \qquad \eta_\alpha = \Psi_\alpha \ (\alpha = 1, \ldots, m), \qquad \eta_t = Y_t \ (t = m+1, \ldots, s)$$

führe man jetzt eine gleichmäßige Bezeichnung der Variabeln ein. Hierdurch und durch (8) geht

$$u\Phi + v\Psi = \sum_{i=0}^{r-1} u\Phi_i X_i + \sum_{i=0}^{r-1} v\Psi_i X_i$$

in $$u\Phi + v\Psi = \sum_{\alpha=1}^{m} (uX_{\alpha-1} + vX_\alpha)\eta_\alpha + \sum_{p=m+1}^{r-1} (u\Phi_p + v\Psi_p) X_p$$

über. Hier sind Φ_p und Ψ_p in $y_1, \ldots, y_s$ und daher auch in $\eta_1, \ldots, \eta_s$ linear; es sei also etwa

$$\Phi_p = \sum_{\alpha=1}^{s} a_{p\alpha}\eta_\alpha, \quad \Psi_p = \sum_{\alpha=1}^{s} b_{p\alpha}\eta_\alpha \quad (p = m+1, \ldots, r-1),$$

wo die a und b Zahlen aus K sind. Danach ist

$$(11) \qquad \begin{aligned} u\Phi + v\Psi &= u\Big(X_0 + \sum_p a_{p1}X_p\Big)\eta_1 + u\sum_{\alpha=2}^{m} X_{\alpha-1}\eta_\alpha \\ &+ u\sum_{\alpha=2}^{m}\sum_p b_{p,\alpha-1}X_p\eta_\alpha + v\sum_{\alpha=1}^{m}\Big(X_\alpha + \sum_p b_{p\alpha}X_p\Big)\eta_\alpha + \varrho + \sigma. \end{aligned}$$

Die Summationen nach p erstrecken sich hier von $m+1$ bis $r-1$; ferner ist $\varrho = u(l_2\eta_2 + \cdots + l_m\eta_m)$, wo die l in den $X_p (p > m)$ linear sind; endlich ist σ eine Form in den

$$X_p, \eta_q (p > m, q > m).$$

Bei der Ableitung von (11) wurden nämlich die Glieder mit $\eta_\alpha (\alpha > m)$, die von Ψ_p herrührten, zu σ geschafft, die Glieder mit $\eta_\alpha (\alpha = 2, \ldots, m)$, die von Φ_p herrührten, zu ϱ und die Glieder mit $\eta_\alpha (\alpha > m)$ wieder zu σ. Endlich addierten wir auf der rechten Seite die dritte Summe und subtrahierten sie von ϱ. Wenden wir jetzt auf (11) die nichtsinguläre Transformation

$$\xi_0 = X_0 + \sum_p a_{p1}X_p, \quad \xi_\alpha = X_\alpha + \sum_p b_{p\alpha}X_p, \quad \xi_p = X_p$$
$$(\alpha = 1, \ldots, m;\ p = m+1, \ldots, r-1)$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

an und setzen mit veränderter Bezeichnung $u\Phi + v\Psi$ an Stelle von σ, so erhalten wir (12); d. h.

Satz 1: φ und ψ seien bilineare Formen in $x_1, \ldots, x_r, y_1, \ldots, y_s$, wo $r \geqq s$, mit Koeffizienten aus K. Für $r = s$ verschwinde die Determinante $|u\varphi + v\psi|$ identisch in u, v. Dann gibt es lineare nichtsinguläre Transformationen der x und solche der y mit Koeffizienten aus K, welche $u\varphi + v\psi$ in

$$(12) \qquad S = \sum_{\alpha=1}^{m} (u\xi_{\alpha-1} + v\xi_\alpha)\eta_\alpha + u\sum_{\alpha=2}^{m} l_\alpha \eta_\alpha + u\Phi + v\Psi$$

überführen. Dabei sind $l_2, \ldots, l_m$ lineare Formen in $\xi_{m+1}, \ldots, \xi_{r-1}$, und Φ und Ψ sind bilineare Formen in $\xi_{m+1}, \ldots, \xi_{r-1}, \eta_{m+1}, \ldots, \eta_s$, alle mit Koeffizienten aus K.

Liegt nun ein Paar λ, μ bilinearer Formen mit Koeffizienten aus K vor, für welches $u\lambda + v\mu$ den Rang R besitzt, so können wir in K lineare Kombinationen φ und ψ von λ, μ angeben, so daß der größte gemeinsame Teiler aller Rreihigen Determinanten von $u\varphi + v\psi$ nicht den Faktor u enthält, also ψ den Rang R besitzt. — Dieses Büschel $u\varphi + v\psi$ bringe man in die Gestalt (12) und bezeichne den Rang von $u\Phi + v\Psi$ mit τ. Dann wird behauptet:

Hilfssatz 4: Der größte gemeinsame Teiler aller τ-reihigen Determinanten von $u\Phi + v\Psi$ ist nicht durch u teilbar.

Bildet man zum Beweise die Matrix M von (12), so werden ihre ersten m Spalten von der Matrix M_1 der Koeffizienten von $\xi_0, \ldots, \xi_{r-1}$ in

$$\frac{\partial S}{\partial \eta_1} = u\xi_0 + v\xi_1, \quad \frac{\partial S}{\partial \eta_2} = u\xi_1 + v\xi_2 + ul_2, \ldots,$$

$$\frac{\partial S}{\partial \eta_m} = u\xi_{m-1} + v\xi_m + ul_m$$

geliefert; da diese offenbar linear unabhängig sind, so hat M_1 den Rang m. Die übrigen $s - m$ Spalten von M werden von der Matrix M_2 der Koeffizienten von $\xi_0, \ldots, \xi_{r-1}$ in den partiellen Ableitungen von $u\Phi + v\Psi$ nach $\eta_{m+1}, \ldots, \eta_s$ geliefert; ihr Rang ist definitionsgemäß gleich τ. Daher können nicht alle $(m + \tau)$reihigen Minoren von M verschwinden, wohl aber alle Minoren höheren Grades; denn sie enthalten mehr als τ Spalten von M_2, verschwinden demnach, wenn man sie nach den Minoren ihrer aus M_2 stammenden Spalten entwickelt. Der Rang von M ist also $m + \tau = R$.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Jede nicht verschwindende $(m+\tau)$reihige Determinante von M enthält genau τ Spalten von M_2 und ist somit eine lineare Funktion gewisser τreihiger Determinanten von M_2 und daher auch von $u\Phi + v\Psi$. Wenn also alle τreihigen Determinanten des letzteren Büschels durch u teilbar wären, so gälte das Gleiche für alle $(m+\tau) = R$reihigen Minoren von M, also auch von S, gegen die Voraussetzung. —

Wenn nun zunächst die Determinante des letzten Teiles $u\Phi + v\Psi$ von (12) nichtidentisch verschwindet (so daß die Form also u. a. eine quadratische Matrix besitzt), so ist sie nach Hilfssatz 4 nicht durch u teilbar, d. h. es ist $|\Psi| \neq 0$. Nach Satz 4 des § 58 gibt es dann in K eine nichtsinguläre lineare Transformation der x und eine solche der y ,welche Φ und Ψ in

$$\varrho = \sum_k \left(\sum_{i=1}^{a_k - 1} x_{k,i} y_{k,i+1} + x_{k,a_k} \sum_{i=1}^{a_k} b_{k,i} y_{k,i} \right),$$
$$\sigma = \sum_k \sum_{i=1}^{a_k} x_{k,i} y_{k,i} \tag{13}$$

überführen. Die dazu nötigen Transformationen lassen jede in der ersten Summe von (12) vorkommende Variable ungeändert und ersetzen die zweite Summe durch $u \sum t_\alpha \eta_\alpha$, wo t_α eine lineare Funktion der $x_{k,i}$ ist. Für $r \geqq s$ können daher φ und ψ rational in

$$J = \sum_{\alpha=1}^{m} \xi_{\alpha-1} \eta_\alpha + \sum_{\alpha=2}^{m} \sum_k \sum_{i=1}^{a_k} d_{k i \alpha} x_{k,i} \eta_\alpha + \varrho$$
$$K = \sum_{\alpha=1}^{m} \xi_\alpha \eta_\alpha + \sigma \tag{14}$$

übergeführt werden.

Verschwindet jedoch die Determinante von $u\Phi + v\Psi$ identisch, so können wir auf dieses Büschel unser Verfahren von $u\varphi + v\psi$ anwenden und es rational in eine Form $R_1 + uP_1 + f_1$ vom Typus (12) oder in die entsprechende Form $S_1 + uQ_1 + f_1$, die man erhält, wenn man ξ und η vertauscht, transformieren. Dabei ist

$$f_1 = u\Phi_1 + v\Psi_1, \quad R_1 = \sum_{\alpha=1}^{m_1} (u\xi_{1,\alpha-1} + v\xi_{1\alpha})\eta_{1\alpha}, \quad P_1 = \sum_{\alpha=2}^{m_1} p_{1\alpha}\eta_{1\alpha},$$
$$S_1 = \sum_{\alpha=1}^{n_1} (u\eta_{1,\alpha-1} + v\eta_{1\alpha})\xi_{1\alpha}, \quad Q_1 = \sum_{\alpha=2}^{n_1} q_{1\alpha}\xi_{1\alpha}.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Fällt f_1 unter den nichtsingulären Fall, so können Φ_1, Ψ_1 rational in Formen vom Typus (13) transformiert werden. Fällt es hingegen unter den singulären Fall, so zeigt eine Fortsetzung unseres Verfahrens, daß f_1 rational in $R_2 + uP_2 + f_2$ oder in $S_2 + uQ_2 + f_2$ transformiert werden kann, wo die Formen entsprechende Typen haben wie oben.

Dieses Verfahren muß ein Ende finden, da die Zahl der Variabeln in $\Phi, \Phi_1, \ldots$ mit jedem Schritt abnimmt.

Wir wollen nun durch Induktion zeigen, daß der mittlere Teil $\sum l_\alpha \eta_\alpha$ in (12) (und entsprechend P_1 oder Q_1, P_2 oder Q_2 usw.) durch weitere Transformationen mit Koeffizienten aus K weggeschafft werden kann, ohne daß dadurch die Summe der übrigen Glieder geändert wird und nehmen dazu an, daß $P_1, Q_1, P_2, Q_2, \ldots$ schon weggeschafft sind.

Wir zeigen zunächst, daß R_1 (und entsprechend R_2 usw.) in der Form eines Gliedes von $u\varrho + v\sigma$ von (13) geschrieben werden kann. In der Tat geht R_1 (bei verändertem Wert von k) durch

$$\xi_{1\,\alpha} = x_{k,\alpha+1} \quad (\alpha = 0, 1, \ldots, m_1), \qquad \eta_{1,\alpha} = y_{k,\alpha+1} \quad (\alpha = 1, \ldots, m_1)$$

und, wenn man $m_1 = a_k - 1$ setzt, in

$$u \sum_{i=1}^{a_k - 1} x_{k,i} y_{k,i+1} + v \sum_{i=1}^{a_k} x_{k,i} y_{k,i}, \tag{15}$$

wo $y_{k1} = 0$, über; wie man sieht, sind die Koeffizienten von u und v Glieder von (13), wenn man dort jedes $b_{ki} = 0$ setzt. Ähnlich hat man in S_1

$$\xi_{1\,\alpha} = x_{k,n_1+1-\alpha} \quad (\alpha = 1, \ldots, n_1), \qquad \eta_{1\,\alpha} = y_{k,n_1+1-\alpha} \quad (\alpha = 0, 1, \ldots, n_1)$$

und $n_1 = a_k - 1$ zu setzen, um es in (15) mit $x_{k,a_k} = 0$ übergehen zu lassen.

Mag daher $u\Phi + v\Psi$ zum singulären Fall zählen oder nicht, auf jeden Fall können wir für $r \geqq s$ das Ausgangspaar φ, ψ auf ein Paar (14) reduzieren, in welchem für gewisse Werte von k entweder x_{k,a_k} oder y_{k1} wegfällt und jedes b_{ki} in (13) und der zweiten Summe von (14) verschwindet.

Es ist jetzt noch zu beweisen, daß wir in (14) auch jedes $d = 0$ setzen dürfen. Wir werden zunächst zeigen, daß wir es im Falle $i < a_k$ dürfen. Wir gehen bei festem k für α induktiv vor. Angenommen, für eine zwischen 2 und m liegende ganze Zahl n, d. h.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$2 \leqq n \leqq m$, sei $d_{kia} = 0$ für $i < a_k$ und $\alpha = 2, \ldots, n-1$. Durch die Transformation[1])

$$\xi_n = X_n + \sum_{i=2}^{a_k} t_{ki} x_{ki}, \quad y_{ki} = Y_{ki} - t_{ki}\eta_n \qquad (i = 2, \ldots, a_k),$$

welche jede der links nicht vorkommenden Variabeln ungeändert läßt, erhalten K bzw. J die Zuwüchse Null bzw.

$$\eta_{n+1} \sum_{i=2}^{a_k} t_{ki} x_{ki} - \sum_{i=1}^{a_k - 1} t_{k,i+1} x_{ki} \eta_n + c x_{k,a_k} \eta_n.$$

(Für die $n = m$ fällt die erste Summe weg.) Setzt man jetzt

$$t_{k,i+1} = d_{ki\,n} \qquad (i = 1, \ldots, a_k - 1),$$

so erhalten wir Formen vom Typus (14), in denen $d_{kia} = 0$ für $i < a_k$, $\alpha = 2, \ldots, n$. Unsere Induktion ist also vollständig, und wir haben jetzt

$$\begin{aligned} J &= \sum_{\alpha=1}^{m} \xi_{\alpha-1}\eta_\alpha + \sum_{\alpha=2}^{m} \sum_{k} e_{k,\alpha} y_{k,a_k} \eta_\alpha + \varrho \\ K &= \sum_{\alpha=1}^{m} \xi_\alpha \eta_\alpha + \sigma. \end{aligned} \tag{16}$$

Wir werden nunmehr zeigen, daß man auch jedes $e_{k\alpha}$ durch Null ersetzen darf. Der Beweis erübrigt sich, wenn ein solches k vorliegt, für welches x_{k,a_k} wegfällt. Wieder gehen wir bei festem k für α induktiv vor und nehmen an, daß für eine gegebene positive ganze Zahl n $(n < m)$ $e_{k\alpha} = 0$ für $\alpha = m, m-1, \ldots, n+2$.

Zunächst sei $n < a_k$. Durch die Transformation

$$\begin{aligned} \xi_{n-j} &= X_{n-j} + t x_{k,a_k-j} && (j = 0, \ldots, n) \\ y_{k,a_k-j} &= Y_{k,a_k-j} - t\eta_{n-j} && (j = 0, \ldots, n-1), \end{aligned} \tag{17}$$

welche die links nicht vorkommenden Variabeln ungeändert läßt, erhalten K bzw. J die Zuwüchse Null bzw.

$$t x_{k,a_k} \eta_{n+1} - t x_{k,a_k} \sum_{j=0}^{n-1} b_{k,a_k-j} \eta_{n-j}. \tag{18}$$

Setzt man $t = -e_{k,n+1}$, so erhält man (16), wo zwar $e_{k\alpha} = 0$ $(\alpha = m, \ldots, n+1)$, wo aber jetzt noch ein neues Glied $c x_{k,a_k} \eta_1$

1) Die Summation hat jedoch schon bei $a_k - 1$ abzubrechen, wenn ein k vorliegt, für welches x_{k,a_k} in (13) und (14) wegfällt. In diesem Falle hat man im Texte $c = 0$ zu setzen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

vorkommt; man kann es indessen beseitigen durch die Transformation $\xi_0 = \Xi_0 - c x_{k,a_k}$. —

Zweitens sei k einer der Werte, für den y_{k1} in (13) nicht verschwindet, und es sei $n \geqq a_k$. Man transformiere wie in (17), nur daß jetzt beide Male $j = 0, \ldots, a_k - 1$. Wieder bleibt K unverändert, während J um (18) zunimmt, wenn j dort die Werte $0, \ldots, a_k - 1$ durchläuft. Dann gehen wir wie im ersten Falle vor.

In beiden Fällen erhalten wir Formen vom Typus (16), in denen jetzt $e_{k\alpha} = 0$ $(\alpha = m, m-1, \ldots, n+1)$. Durch Induktion für n erhalten wir die Gestalt (16), worin jedes $e_{k\alpha} = 0$. —

Drittens nehme k einen Wert an, für den in (16) y_{k1} wegfällt und jedes $b_{ki} = 0$ wird. Dann ist, wie wir sehen werden, $m < a_k$, also $n < a_k$, so daß der zweite Fall ausgeschlossen ist. Zum Beweise setze man

$$S = uJ + vK, \quad \sum_\alpha = \frac{\partial S}{\partial \xi_\alpha} \quad (\alpha = 0, \ldots, m). \qquad S_{ki} = \frac{\partial S}{\partial x_{ki}} \quad (i = 1, \ldots, a_k).$$

Nach (16) und (13) ist demnach

$$\sum_0 = u\eta_1, \quad \sum_\alpha = u\eta_{\alpha+1} + v\eta_\alpha \quad (\alpha = 1, \ldots, m-1), \tag{19}$$

$$\sum_m = v\eta_m,$$

oder nach den η aufgelöst

$$u^{\alpha+1}\eta_{\alpha+1} = \sum_{j=0}^{\alpha} (-1)^j u^{\alpha-j} v^j \sum_{\alpha-j} \quad (\alpha = 0, \ldots, m-1). \tag{20}$$

Eliminiert man den aus der letzten Gleichung von (19) resultierenden Wert von η_m, so folgt

$$u^m \sum_m = \sum_{i=1}^{m} (-1)^{i-1} u^{m-i} v^i \sum_{m-i}. \tag{21}$$

Ferner ist

$$S_{ki} = u y_{k,i+1} + v y_{ki} \quad (i < a_k), \quad S_{k,a_k} = u \sum_{\alpha=2}^{m} e_{k\alpha}\eta_\alpha + v y_{k,a_k}, \tag{22}$$

woraus, da $y_{k1} = 0$, folgt, daß

$$u^{i+1} y_{k,i+2} = \sum_{j=0}^{i} (-1)^j u^{i-j} v^j S_{k,i+1-j} \quad (i = 0, \ldots, a_k - 2). \tag{23}$$

Wie man aus (20) und (23) sieht, sind $u^t \eta_t$ und $u^t y_{k,t+1}$ lineare Funktionen der Σ und S, deren Koeffizienten Polynome in u, v

Digitized by Google Original from UNIVERSITY OF MICHIGAN

vom Grade $t-1$ sind. Nimmt man jetzt $m \geqq a_k$ an, so erhält man durch Multiplikation der letzten Gleichung (22) mit u^{m-1}

$$(24) \qquad u^{m-1} S_{k,a_k} = \sum_{\alpha=2}^{m} e_{k\alpha} u^{m-\alpha} u^{\alpha} \eta_\alpha + v u^{m-a_k} u^{a_k-1} y_{k,a_k}.$$

Nach der eben gemachten Bemerkung liefert dies eine lineare Beziehung zwischen den ersten Ableitungen von S, deren Koeffizienten in u, v vom Grade $m-1$ sind. Dies widerspricht aber, da S_{k,a_k} rechts nicht vorkommt, der Definition von m. — Damit ist unsere Annahme $m \geqq a_k$ als falsch erkannt und es muß daher $m < a_k$, also auch $n < a_k$, so daß wir das Ergebnis des ersten Falles übertragen können.

Damit haben wir den vollständigen Beweis dafür, daß wir in (14) jedes $d = 0$ setzen können. In dem folgenden Satz führen wir die Formen R_i und S_i, die wir bisher mit $u\varrho + v\sigma$ vereinigt hatten, besonders an. Für jedes i ist nur eines der Paare R_i und S_i eine Komponente der kanonischen Form. — Schließlich ändern wir noch die Bezeichnung der in S_j vorkommenden Variabeln.

Satz 2: φ und ψ seien bilineare Formen mit Koeffizienten in einem Körper K und ψ[1]) habe denselben Rang wie $f = u\varphi + v\psi$. Im singulären Falle kann f durch nichtsinguläre lineare Transformationen mit Koeffizienten aus K auf die Gestalt

$$S = \sum R_i + \sum S_j + u\varrho + v\sigma$$

gebracht werden, wo ϱ und σ durch (13) gegeben sind und

$$(25) \quad R_i = \sum_{\alpha=1}^{m_i} (u\xi_{i,\alpha-1} + v\xi_{i\alpha})\eta_{i\alpha}, \quad S_j = \sum_{\alpha=1}^{n_j} (uY_{j,\alpha-1} + vY_{j\alpha})X_{j\alpha}.$$

Keine zwei der Formen $R_1, R_2, \ldots, S_1, S_2, \ldots, u\varrho + v\sigma$, haben eine Variable gemeinsam, während alle Variabeln in K linear unabhängig sind. —

Wir werden nunmehr zeigen, daß die von 1 verschiedenen invarianten Faktoren von S mit denen von $u\varrho + v\sigma$ zusammenfallen. Bezeichnet d die Ordnung der in u, v nicht identisch verschwindenden Determinante D von $u\varrho + v\sigma$ und ist $t = \sum m_i + \sum n_i$, so ist, wie wir sehen werden, der Rang von M gleich $d + t$. In M

1) Wir sahen, daß man dies durch passende lineare Kombination der φ und ψ mit Koeffizienten aus K immer erreichen kann.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

steht der Koeffizient eines Produktes $\xi\eta$ in dem Schnitt der zu ξ gehörenden Reihe $[\xi]$ mit der zu η gehörenden Spalte $[\eta]$. Ähnlich für XY.

Zunächst tilge man die Zeilen $[\xi_{i,m_i}]$ und die Spalten $[Y_{j,n_j}]$, die in den R_i bzw. S_j zu den ξ bzw. Y mit maximalem zweitem Index gehören. Wir erhalten eine quadratische Matrix, in welcher (abgesehen von Elementen von D) jedes Diagonalelement gleich u ist und in welcher die rechts (links) von diesen u stehenden Elemente bei R_i (S_j) verschwinden; ihre Determinante ist daher gleich $u^t D$.

Sodann tilge man die Zeilen $[\xi_{i0}]$ und die Spalten $[Y_{j0}]$. Wieder erhalten wir eine quadratische Matrix, in der jetzt (abgesehen von Elementen von D) jedes Diagonalelement gleich v ist und in der die links (rechts) von diesen v stehenden Elemente bei R_i (S_j) verschwinden; ihre Determinante ist daher gleich $v^t D$.

Demnach ist D der größte gemeinsame Teiler aller $(d+t)$-reihigen Determinanten von M. Dies liefert (vgl. Kap. V, 43) den

Hilfssatz 5: Die von 1 verschiedenen invarianten Faktoren von S fallen mit denen von $u\varrho + v\sigma$ zusammen.

Daher sind ϱ und σ schon durch die invarianten Faktoren von $u\varphi + v\psi$ eindeutig bestimmt. —

Die Variabeln ξ, X, x der ersten Reihe in S sind nach Satz 2 linear unabhängig, desgleichen die Variabeln η, Y, y der zweiten Reihe. Setzt man $W = u\varrho + v\sigma$, so kommt keine Variable in zwei der Formen R_i, S_j, W gemeinsam vor. Daher ist eine lineare Funktion $[S]$ der ersten Ableitungen von $S = W + \sum R_i + \sum S_j$ nach den Variablen einer der beiden Reihen eine Summe von linearen Funktionen $[W], [R_1], [R_2], \ldots, [S_1], \ldots$ der ersten Ableitungen von $W, R_1, R_2, \ldots$ nach ihren eigenen Variablen. Außerdem folgt aus $[S] = 0$, daß $[W] = 0$, $[R_1] = 0, \ldots$ Da $|W|$ nun nicht identisch verschwindet, so kann $[W]$ nur verschwinden, wenn alle seine Koeffizienten gleich Null sind.

Unterdrücken wir bei m_i und den Variablen in R_i den Index i und schreiben für $\frac{\partial R_i}{\partial \xi_\alpha}$ kurz $\sum_\alpha$, so haben wir die Beziehungen (19)—(21). Da aber $\sum_0, \ldots, \sum_{m-1}$ linear unabhängig sind, so erhält man jede lineare Beziehung zwischen den Σ durch Multiplikation von (21) mit einer Funktion von u und v.

Nun sind aber die ersten Ableitungen von R_i nach den η_{ia} offenbar linear unabhängig; da ferner R_i in S_i übergeht, wenn man ξ, η, m mit Y, X, n vertauscht, so ergibt sich

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Hilfssatz 6: Als vollständiges System linear unabhängiger Beziehungen zwischen den ersten Ableitungen von S nach den Variabeln ξ, X, x der ersten Reihe kann man die Beziehungen

$$u^{m_i} \cdot \frac{\partial S}{\partial \xi_{i,m_i}} = \sum_{j=1}^{m_i} (-1)^{j-1} u^{m_i-j} v^j \frac{\partial S}{\partial \xi_{i,m_i-j}} \tag{26}$$

annehmen, wo i die gleichen Werte wie der Index von R_i durchläuft. m_i ist hier der Minimalgrad der Koeffizienten (in u, v) irgendeiner linearen Beziehung zwischen den ersten Ableitungen von S nach den Variablen ξ_i von R_i. — Ähnlich ist n_j der Minimalgrad der Koeffizienten (in u, v) irgendeiner linearen Beziehung zwischen den ersten Ableitungen von S nach den Variablen Y_j von S_j. Diese Beziehungen vom Minimalgrade bilden ein vollständiges System unabhängiger linearer Beziehungen zwischen den ersten Ableitungen von S nach den Variablen der zweiten Reihe. —

R_i und S_j sind durch die Minimalgrade m_i und n_j eindeutig bestimmt. Nach Hilfssatz 1 haben sie für $u\varphi + v\psi$ denselben Wert wie für die kanonische Form S, sind also numerische Invarianten. Sie heißen die Minimalgradzahlen von $u\varphi + v\psi$ oder von S.

Liegen jetzt zwei Paare bilinearer Formen — φ, ψ und λ, μ — aus K vor, deren jedes unsere Anfangsbedingung erfüllt und die in Satz 2 erwähnte, den Rang betreffende Eigenschaft besitzt, so folgt aus Hilfssatz 5 und 6 und den darauf folgenden Bemerkungen, daß die Paare dann und nur dann dieselbe kanonische Form haben (und daher dann und nur dann in K äquivalent sind), wenn sie dieselben Minimalgradzahlen und dieselben invarianten Faktoren besitzen. —

Wir müssen dieses Resultat noch für den Fall beweisen, wo die beiden den Formen auferlegten Beschränkungen wegfallen.

f und g seien bilineare Formen aus K, und es sei $|uf + vg| \equiv 0$. Wir dürfen (evtl. nach Hinzufügen von verschwindenden Koeffizienten) voraussetzen, daß die Anzahl der Variabeln X_i und Y_i beide Male gleich n ist. Ist dann τ der Rang von $h = uf + vg$, so gibt es genau $n - \tau$ unabhängige lineare Beziehungen zwischen den n Ableitungen von h nach den X_i (oder Y_i). Wir denken uns diese so gewählt, daß sie in u, v von möglichst niederem Grade sind. Diese Gradzahlen seien der Größe nach $M_1, \ldots, M_{n-\tau}$ (oder $N_1, \ldots, N_{n-\tau}$).

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Es sei z. B. $f = X_1 Y_3 + X_3 Y_1$, $g = X_2 Y_3 + X_3 Y_2$. Dann hat h die Matrix

$$\begin{pmatrix} 0 & 0 & u \\ 0 & 0 & v \\ u & v & 0 \end{pmatrix}$$

vom Range 2. Demnach ist $v h_1 - u h_2 \equiv 0$ die einzige lineare Beziehung zwischen den Ableitungen h_1, h_2, h_3 von h nach X_1, X_2, X_3. Die Minimalgradzahlen sind $M_1 = 1$, $N_1 = 1$. Da unter den zweireihigen Determinanten eine gleich $-u^2$, eine andere gleich $-v^2$ ist, so ist ihr größter gemeinsamer Teiler gleich 1. Die Matrix hat also keinen anderen invarianten Faktor als 1.

Sind die ϱ ersten M_i und die σ ersten N_i Null (so daß alle anderen positiv sein müssen), so können wir f, g in ein Paar φ, ψ überführen, in dem nur $r = n - \varrho$ Variabeln x_i und nur $s = n - \sigma$ Variablen y_i vorkommen (Hilfssatz 2). φ, ψ genügen dann unserer Voraussetzung, daß sie sich nicht rational in ein Formenpaar transformieren lassen, welches weniger als r Variablen x_i oder s Variablen y_i enthält.

Da nach Hilfssatz 1 M_i und N_i invariant gegenüber jeden linearen Transformation der X oder Y sind, so sind die positiven der M_i und N_i nichts anderes als die obigen m_i und n_i von φ und ψ. Auch sie heißen daher die Minimalgradzahlen des Paares f, g. —

Man führe die linearen Kombinationen

$$\varphi' = a\varphi + b\psi, \quad \psi' = c\varphi + d\psi \qquad (ad - bc = 1) \tag{27}$$

ein und setze $\chi = u\varphi + v\psi$, $\chi' = u'\varphi' + v'\psi'$. Dann ist $\chi = \chi'$, wenn

$$u' = du - cv, \quad v' = -bu + av. \tag{28}$$

Vor Hilfssatz 4 wählten wir a, b, c, d so, daß der größte gemeinsame Teiler aller Rreihigen Minoren von χ' nicht durch u' teilbar war, wo R der Rang von χ und daher auch von ψ' ist.

λ, μ sei ein anderes Paar bilinearer Formen in $x_1, \ldots, x_r$, $y_1, \ldots, y_s$ mit Koeffizienten aus K, welches dieselben Minimalgradzahlen und dieselben invarianten Faktoren wie das Paar φ, ψ hat. Mit denselben a, b, c, d wie in (27) setze man

$$\lambda' = a\lambda + b\mu, \quad \mu' = c\lambda + d\mu, \quad \omega = u\lambda + v\mu,$$
$$\omega' = u'\lambda + v'\mu'.$$

Da χ' und ω' durch (28) in χ und ω transformiert werden, so stimmen sie in den Minimalgradzahlen, in den invarianten Faktoren

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

und im besonderen im Rang R und in dem größten gemeinsamen Teiler ihrer Rreihigen Determinanten überein. Demnach ist μ' auch vom Range R.

Satz 2 und die auf die Hilfssätze 5 und 6 folgenden Bemerkungen zeigen, daß χ' und ω' dieselbe kanonische Form haben und daher in K äquivalent sind. Das Gleiche gilt daher für die Paare φ, ψ und λ, μ; sie sind ebenfalls in K äquivalent. — Damit haben wir den vollständigen Beweis des fundamentalen Satzes:

Satz 3: Stimmen im singulären Falle für zwei Paare bilinearer Formen in den gleichen $n + n$ Variabeln mit Koeffizienten aus K die invarianten Faktoren und die Minimalgradzahlen überein, so sind sie in K äquivalent, und umgekehrt.

Das kanonische Paar zeigt, daß man als Minimalgradzahlen und invariante Faktoren irgendwelche Werte (wo bei letzteren jeder Faktor im nächstfolgenden enthalten ist) vorschreiben kann.

65. Paare symmetrischer bilinearer Formen im singulären Falle. Unsere Ausgangsform sei

$$f = \sum_{i,j=1}^{n} a_{ij} x_i x_j, \quad a_{ij} = a_{ji} \tag{29}$$

mit der symmetrischen Matrix $A = (a_{ij})$. Wenn nun die $\frac{\partial f}{\partial x_i}$ voneinander abhängen, d. h. wenn

$$\sum_{i=1}^{n} c_i \frac{\partial f}{\partial x_i} \equiv 0 \tag{30}$$

(wo die c keine Funktionen der x und y sind), so ist

$$\sum_{j=1}^{n} c_j a_{ij} = 0 \qquad (j = 1, \ldots, n), \tag{31}$$

d. h. es ist auch $\sum c_i \cdot \frac{\partial f}{\partial y_i} \equiv 0$. Setzt man jetzt $f = u\varphi + v\psi$, so stimmen also die Minimalgradzahlen M_i und N_i des Paares φ, ψ miteinander überein.

Betrachtet man zwei Paare von Formen φ, ψ und λ, μ, deren $n$reihige Matrizen A, B, C, D symmetrisch sind, und nimmt an, daß $u\varphi + v\psi$ und $u\lambda + v\mu$ dieselben invarianten Faktoren und dieselben Minimalgradzahlen M_i (und also auch N_i) haben, so

Digitized by Google Original from UNIVERSITY OF MICHIGAN

sind nach Satz 3 diese Paare äquivalent, so daß nichtsinguläre $n$reihige Matrizen P, Q existieren, für welche

$$C = PAQ, \quad D = PBQ.$$

Nach 61. gibt es daher eine nichtsinguläre $n$reihige Matrix M, für die

$$C = M'AM, \quad D = M'BM,$$

so daß φ und ψ durch die lineare Transformation E der x und y in λ und μ übergeht. Da sich der Beweis auch umkehren läßt, so haben wir:

Satz 4: Im singulären Falle sind zwei Paare symmetrischer bilinearer Formen dann und nur dann gegenüber einer nichtsingulären linearen Transformation der x und y äquivalent, wenn sie dieselben invarianten Faktoren und dieselben Minimalgradzahlen M_i (die hier mit den N_i identisch sind) besitzen.

Sucht man eine kanonische Form für ein solches Paar φ, ψ, so hat man zu bedenken, daß die Zahl der verschwindenden M_i gleich der Zahl der x (oder y) ist, welche durch lineare Transformationen weggebracht werden können. Jedes $M_i \neq 0$ bezeichne man mit m_i; ihre Anzahl sei p. Benutzt man die Bezeichnungen des Satzes 2, so ist

$$C = \sum_{i=1}^{p} T_i + u\gamma + v\delta$$

eine kanonische Form; dabei ist $T_i = R_i + S_i$, ferner ist für S_i $n_i = m_i$, endlich ist $u\gamma + v\delta$ symmetrisch, hat eine in u, v nichtidentisch verschwindende Determinante und hat dieselben invarianten Faktoren wie $u\varphi + v\psi$.

Um die Symmetrie jedes T_i hervorzuheben, ersetze man ξ_α durch x_α, X_α durch $x_{m_i+\alpha}$, Y_α durch y_α und η_α durch $y_{m_i+\alpha}$. Dann haben wir

Satz 5: Im singulären Falle läßt sich jedes Paar symmetrischer bilinearer Formen durch eine nichtsinguläre lineare Transformation der x und die kogrediente Transformation der y auf ein kanonisches Paar zurückführen, welches die Koeffizienten von u und v in

$$\sum T_i + u\gamma + v\delta \qquad \textit{darstellt, wo}$$

$$T_i = \sum_{\alpha=1}^{m_i} [(u x_{i,\alpha-1} + v x_{i\alpha}) y_{i,m_i+\alpha} + (u y_{i,\alpha-1} + v y_{i\alpha}) x_{i,m_i+\alpha}]$$

in seinen $2m_i + 1$ Paaren von Variabeln symmetrisch ist, während γ, δ das kanonische Paar im nichtsingulären Fall ist. (Vgl. 63.)

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

66. **Paare quadratischer Formen im singulären Falle.** $f = u\varphi + v\psi$ sei vom Typus (29). Ihr entspricht die quadratische Form $q = \sum a_{ij} x_i x_j$. Dann ist nach (31)

$$\frac{\partial q}{\partial x_i} = 2\sum_{j=1}^{n} a_{ij} x_j, \quad \sum_{i=1}^{n} c_i \frac{\partial q}{\partial x_i} = 2\sum_{j=1}^{n}\Big(\sum_{i=1}^{n} c_i a_{ij}\Big) x_j = 0.$$

Daher folgt aus jeder linearen Beziehung (30) zwischen den n Ableitungen von f nach den x_i, deren Koeffizienten c_i Polynome in u, v sind, eine lineare Beziehung mit denselben Koeffizienten c_i zwischen den Ableitungen von q und umgekehrt. Die Minimalgradzahlen $M_i = N_i$ von f stimmen demnach mit denen von q überein. Nach Satz 4 und der Folgerung in 33. haben wir also:

Satz 6: Im singulären Falle sind zwei Paare quadratischer Formen dann und nur dann äquivalent, wenn sie dieselben invarianten Faktoren und dieselben Minimalgradzahlen M_i haben.

Aus Satz 5 erhalten wir jetzt ein kanonisches Paar quadratischer Formen, wenn wir y mit x zusammenfallen lassen:

$$(32) \quad \gamma + 2\sum_{i=1}^{p}\sum_{\alpha=1}^{m_i} x_{i,\alpha-1} x_{i,m_i+\alpha}, \quad \delta + 2\sum_{i=1}^{p}\sum_{\alpha=1}^{m_i} x_{i\alpha} x_{i,m_i+\alpha},$$

wo γ, δ ein kanonisches Paar im nichtsingulären Fall ist (vgl. 63.). Im besonderen gibt es ein Paar quadratischer Formen mit vorgeschriebenen invarianten Faktoren und vorgeschriebenen Minimalgradzahlen.

Als Beispiel von (32) diene $2x_0x_2, 2x_1x_2$. Wir haben dann

$$v\frac{\partial f}{\partial x_0} - u\frac{\partial f}{\partial x_1} \equiv 0, \quad f = 2ux_0x_2 + 2vx_1x_2.$$

Hier gibt es nur eine einzige Minimalgradzahl $M_1 = 1$ und keinen invarianten Faktor.

67. **Weitere Anwendungen der Matrizentheorie.** Die Hurwitzsche Identität, welche das Produkt einer Summe von p Quadraten und einer Summe von n Quadraten darstellt als Summe von n Quadraten.[1])

1) Betr. des Falles $p = n$ vergleiche man Dickson, Annals of Math. 20, 1919, p. 160. — Radon, Abhandl. Math. Hamburger Univ. 1, 1921, pp. 1—14. Er fand im Falle reeller Matrizen die Maximalzahl p für ein gegebenes n. — Eine Verallgemeinerung auf Formen beliebiger Ordnung fand Dickson, Congrès International des Mathématiciens, Straßburg, 1920, pp. 215—30; Comptes Rendus Paris 172, 1921, pp. 636—40, p. 1262.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Frobeniussche Theorie der Matrizen, deren Elemente Polynome einer Variablen sind. Anwendung auf die Äquivalenz von Paaren bilinearer Formen.[1])

Weierstraß gab eine einfache Anwendung der Theorie der Paare bilinearer Formen auf die Integration eines Systems von n linearen Differentialgleichungen erster Ordnung in n Variabeln mit konstanten Koeffizienten.[2])

---

1) Vgl. Dickson, Algebren und ihre Zahlentheorie, übersetzt von Burckhardt und Schubarth, Zürich 1926, pp. 219—32.

2) Berliner Abhandlungen 1875; Werke II, pp. 75—76.

Digitized by Google

Original from UNIVERSITY OF MICHIGAN

ACHTES KAPITEL.

HAUPTEIGENSCHAFTEN DER SUBSTITUTIONS-GRUPPEN.

Wir werden hier in Verbindung mit der Lösung der Gleichungen dritten und vierten Grades auf sehr konkrete und natürliche Weise die Hauptbegriffe der Substitutionen- und Gruppentheorie entwickeln. Dadurch wird der Leser schon gleich zu Anfang in die Gründe, die zu jenen Begriffen geführt haben, einen Einblick bekommen. Die ganze Darstellung ist durch zahlreiche Beispiele erläutert, die diese etwas abstrakten Gedanken mundgerecht machen sollen.

68. Kubische Gleichungen. Von den mannigfachen Methoden zur Lösung der Gleichung

$$x^3 + bx^2 + cx + d = 0 \tag{1}$$

werden wir hier diejenige Methode entwickeln, welche am besten unsere spätere Theorie der Lösung von Gleichungen beliebigen Grades vorbereitet. — Sind x_1, x_2, x_3 die Wurzeln, so ist

$$\begin{aligned} \sum x_1 &\equiv x_1 + x_2 + x_3 = -b \\ \sum x_1 x_2 &\equiv x_2 x_3 + x_3 x_1 + x_1 x_2 = +c \\ \sum x_1 x_2 x_3 &= -d. \end{aligned} \tag{2}$$

Bezeichnet ω eine imaginäre dritte Einheitswurzel, so ist

$$\omega^2 + \omega + 1 = 0, \quad \omega^3 = 1. \tag{3}$$

Wir gehen nun darauf hinaus, nicht zuerst die Werte der Wurzeln selbst zu berechnen, sondern die Werte gewisser linearer Kombinationen, aus denen sich die Wurzeln dann hinterher leicht bestimmen lassen. Als solche Kombinationen nehmen wir $-b$ (als Summe der Wurzeln) und die beiden Funktionen

$$\varphi = x_1 + \omega x_2 + \omega^2 x_3, \quad \psi = x_1 + \omega^2 x_2 + \omega x_3. \tag{4}$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Addieren wir nämlich die drei Gleichungen, so erhalten wir den Wert von $3x_1$, multiplizieren wir sie der Reihe nach mit $\omega^2, \omega, 1$ bzw. $\omega, \omega^2, 1$ und addieren jedesmal, so erhalten wir wegen (3)

$$(5)\qquad x_1 = \frac{1}{3}(\varphi + \psi - b), \quad x_2 = \frac{1}{3}(\omega^2\varphi + \omega\psi - b),$$
$$x_3 = \frac{1}{3}(\omega\varphi + \omega^2\psi - b).$$

Es kommt jetzt also nur noch darauf an, die Werte von φ und ψ zu berechnen. Dazu benutze man die Entwicklungen

$$(6)\qquad \begin{aligned}\varphi\psi &= \sum x_1^2 + (\omega + \omega^2)\sum x_1 x_2\\ &= \left(\sum x_1\right)^2 - 3\sum x_1 x_2 = A = b^2 - 3c,\end{aligned}$$

$$(7)\qquad \begin{aligned}\varphi^3 + \psi^3 &= 2\sum x_1^3 - 3\sum x_1^2 x_2 + 12\, x_1 x_2 x_3\\ &= 2\left(\sum x_1\right)^3 - 9\sum x_1 \cdot \sum x_1 x_2 + 27\, x_1 x_2 x_3 = B\\ &= -2b^3 + 9bc - 27d.\end{aligned}$$

$$(\varphi^3 - \psi^3)^2 = (\varphi^3 + \psi^3)^2 - 4\varphi^3\psi^3 = B^2 - 4A^3.$$

Daher ist $\varphi^3 - \psi^3$ eine der beiden Quadratwurzeln von $B^2 - 4A^3$. Durch Wahl einer bestimmten Wurzel erhalten wir nach (7):

$$(8)\qquad \varphi^3 = \frac{1}{2}\left[B + (B^2 - 4A^3)^{\frac{1}{2}}\right] = g$$
$$\psi^3 = \frac{1}{2}\left[B - (B^2 - 4A^3)^{\frac{1}{2}}\right] = h.$$

Die Kubikwurzeln φ und ψ von g und h müssen wegen (6) so gewählt werden, daß $\varphi\psi = A$ wird. D. h. wir wählen für φ irgendeine der drei Wurzeln von g und bestimmen ψ aus $\frac{A}{\varphi}$.

Ist φ eine der Wurzeln von g, so sind die beiden anderen gleich $\omega\varphi$ und $\omega^2\varphi$. So erhalten wir die Funktionen

$$(9)\qquad \varphi_1 = \omega\varphi = x_3 + \omega x_1 + \omega^2 x_2$$
$$\psi_1 = \omega^2\psi = x_3 + \omega x_2 + \omega^2 x_1$$

$$(10)\qquad \varphi_2 = \omega^2\varphi = x_2 + \omega x_3 + \omega^2 x_1$$
$$\psi_2 = \omega\psi = x_2 + \omega x_1 + \omega^2 x_3. —$$

Ersetzt man in (5) φ und ψ durch $\omega\varphi$ bzw. $\omega^2\psi$, so wird dadurch x_2 durch x_1, x_1 durch x_3, x_3 durch x_2 ersetzt. Diese Operation heißt

Digitized by Google Original from UNIVERSITY OF MICHIGAN

eine Substitution der Wurzeln (oder Buchstaben) x_1, x_2, x_3 und wird mit $(x_1 x_3 x_2)$ bezeichnet. Dieser sog. Zyklus besagt, daß jeder Buchstabe durch den auf ihn folgenden ersetzt wird, der letzte dann wieder durch den ersten (hier x_1).

Ersetzt man andererseits in (5) φ und ψ durch $\omega^2\varphi$ bzw. $\omega\psi$, so ist dies gleichbedeutend mit der Ausübung der Substitution $(x_1 x_2 x_3)$.

Hätten wir die andere Quadratwurzel von $B^2 - 4A^3$ gewählt, so hätten wir $\varphi^3 = h$, $\psi^3 = g$ an Stelle von (8) erhalten. Diese Vertauschung von φ und ψ hat in (5) dieselbe Wirkung wie die Substitution $(x_2 x_3)$, welche x_2 mit x_3 vertauscht und x_1 ungeändert läßt. Ersetzt man in (5) φ durch $\omega\psi$ und ψ durch $\omega^2\varphi$ bzw. φ durch $\omega^2\psi$ und ψ durch $\omega\varphi$, so wird dadurch die Substitution $(x_1 x_2)$ bzw. $(x_1 x_3)$ induziert.

Das Wichtigste dieser Resultate können wir folgendermaßen zusammenstellen: Haben wir durch bestimmte Wahl der Quadratwurzel in (8) und durch Wahl der Kubikwurzel von g einen festen Wert von φ $\left(\text{und daher auch von } \psi = \frac{A}{\varphi}\right)$ gefunden, so daß die Formeln (5) bestimmte Werte für x_1, x_2, x_3 liefern, dann führt eine andere Wahl der Quadrat- oder Kubikwurzel auf neue Werte von x_1, x_2, x_3, die aber aus den früheren durch eine Substitution hervorgehen. — Dieses Resultat war auch vorauszusehen, denn wenn wir aus den Koeffizienten einer Gleichung die Wurzeln berechnen, so steht es uns frei, diese irgendwie mit x_1, x_2, x_3 zu benennen.

Übung: Bestätige an den linearen Funktionen (4), (9), (10), daß die Substitution $(x_1 x_3 x_2)$ bzw. $(x_1 x_2 x_3)$ φ und ψ durch φ_1 und ψ_1 bzw. φ_2 und ψ_2 ersetzt, während durch $(x_2 x_3)$ φ und ψ, durch $(x_1 x_3)$ φ_1 und ψ_1, durch $(x_1 x_2)$ φ_2 und ψ_2 vertauscht werden. Auch wird φ und ψ durch $(x_1 x_2)$ bzw. $(x_1 x_3)$ in ψ_2 und φ_2 bzw. ψ_1 und φ_1 übergeführt.

69. Diskriminante einer kubischen Gleichung. Als Diskriminante Δ einer kubischen Gleichung, in der x^3 den Koeffizienten 1 hat, definiert man das Produkt der Quadrate der Wurzeldifferenzen. Ihr Verschwinden ist notwendig und hinreichend dafür, daß die Gleichung eine mehrfache Wurzel hat. Wir werden die Diskriminante mittels des in 68. aufgestellten Wertes $B^2 - 4A^3$ von $(\varphi^3 - \psi^3)^2$ berechnen. Da $1, \omega, \omega^2$ die kubischen Einheitswurzeln sind, so haben wir

$$z^3 - 1 \equiv (z - 1)(z - \omega)(z - \omega^2).$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Daher ist auch

$$\varphi^3 - \psi^3 = (\varphi - \psi)(\varphi - \omega\psi)(\varphi - \omega^2\psi).$$

Aus (4), (9), (10) ergibt sich nun

$$\begin{aligned} \varphi - \psi &= (\omega - \omega^2)(x_2 - x_3) \\ \varphi - \omega\psi &= (1 - \omega)(x_1 - x_2) \\ \varphi - \omega^2\psi &= (1 - \omega^2)(x_1 - x_3). \end{aligned} \tag{11}$$

Wir suchen das Produkt der Quadrate der drei Ausdrücke in (11). Da wegen (3)

$$(\omega - \omega^2)^2 = -3, \quad (1 - \omega)(1 - \omega^2) = 3,$$

so ist $B^2 - 4A^3 = -27\Delta$, d. h.

$$\Delta = 18bcd - 4b^3d + b^2c^2 - 4c^3 - 27d^2. \tag{12}$$

Übungen: 1. Die Diskriminante von $x^3 + cx + d = 0$ ist $-4c^3 - 27d^2$.

2. Zeige durch Berechnung der Diskriminante, daß $x^3 - 27x + 54 = 0$ eine mehrfache Wurzel hat.

3. Die Diskriminante Δ von $ax^3 + bx^2 + cx + d = 0$ wird als a^4P definiert, wo P das Produkt der Quadrate der Wurzeldifferenzen bezeichnet, so daß P aus (12) durch Ersetzen von b, c, d durch $\frac{b}{a}$, $\frac{c}{a}$, $\frac{d}{a}$ hervorgeht. Man zeige, daß $\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$.

4. Man zeige mittels (19) aus Kap. I, daß $\Delta = -27D$, wenn D die Diskriminante der entsprechenden kubischen Form $ax^3 + bx^2y + cxy^2 + dy^3$ bezeichnet.

5. Man bestätige mit (11), daß für $\Delta \neq 0$ und $A \neq 0$ (also auch $\varphi \neq 0$, $\psi \neq 0$) die sechs Funktionen (4), (9), (10) sechs verschiedene Werte besitzen. In der Übung in 68. gaben wir eine Substitution an, welche φ durch irgendeine der fünf anderen Funktionen ersetzt. Die identische Substitution, die jedes x_i ungeändert läßt, ändert auch φ nicht. Weil daher φ durch die 6 Substitutionen der 3 Wurzeln in sechs Funktionen, deren Werte alle von einander verschieden sind, übergeführt wird, so heißt es eine sechswertige Funktion.

6. Zeige, daß ψ ebenfalls eine sechswertige Funktion ist. Warum ergibt sich jetzt ohne Berechnung, daß auch jede der 4 Funktionen (9) und (10) sechswertig ist?

70. Allgemeine Substitutionen. Die Operation s, welche x_1 durch x_a, x_2 durch x_b, ..., x_n durch x_l ersetzt, wo die $a, b, \ldots, l$ eine Permutation von $1, 2, \ldots, n$ bilden, heißt eine **Substitution** von $x_1, \ldots, x_n$. Sie wird mit

$$s = \begin{pmatrix} x_1 x_2 \ldots x_n \\ x_a x_b \ldots x_l \end{pmatrix} = \begin{pmatrix} 1\,2 \ldots n \\ a\,b \ldots l \end{pmatrix} \tag{13}$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

bezeichnet. Da die Ordnung der Spalten unwesentlich ist, können wir sie irgendwie vertauschen, ohne daß sich s ändert.

Jeder Permutation $a, b, \ldots, l$ von $1, 2, \ldots, n$ entspricht eine und nur eine Substitution. Daher ist die Zahl der Substitutionen von n Buchstaben gleich $n!$.

Anstelle der zweireihigen Bezeichnung (13) wendet man oft die einreihige Bezeichnung der Zyklen (vgl. 68.) an. Die Beziehung zwischen beiden Arten der Bezeichnung geht aus den folgenden Substitutionen hervor:

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix} = (123), \qquad \begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (123)\,(45).$$

71. Das Produkt von Substitutionen. Wenn durch (13) eine Substitution s und wenn außerdem eine andere Substitution t gegeben ist, so können wir die Spalten von t so permutieren, daß die Elemente ihrer oberen Reihe gleich den entsprechenden Elementen der unteren Reihe von s sind. Wenn also nach s die Substitution

$$t = \begin{pmatrix}a & b & \ldots & l\\ \alpha & \beta & \ldots & \lambda\end{pmatrix} \tag{14}$$

ausgeübt wird, so hat dies denselben Erfolg wie die einzige Substitution

$$p = \begin{pmatrix}1 & 2 & \ldots & n\\ a & \beta & \ldots & \lambda\end{pmatrix}, \tag{15}$$

welche das Produkt von s und t heißt: $p = st$ (das Wort „Produkt" wird hier im Sinne von „Resultante" gebraucht).

Wir können daher leicht das Produkt von Substitutionen, die in Zyklen ausgedrückt sind, finden. Z. B.

$$(12)\,(34)\cdot(23) = (1342), \quad (23)\cdot(12)\,(34) = (1243).$$

Um das erste Produkt zu finden, beachte man, daß der erste Faktor 1 durch 2 und der zweite Faktor 2 durch 3, also ihr Produkt 1 durch 3 ersetzt usw. Wie man sieht, ist die Multiplikation der Substitutionen nicht immer kommutativ.

Besteht eine Substitution aus zwei oder mehr Zyklen, die kein Element gemeinsam haben, so kann sie als Produkt von kommutativen zyklischen Substitutionen, deren jede aus einem einzigen Zyklus besteht, aufgefaßt werden. Z. B. $(12)\,(34) = (12)\cdot(34) = (34)\cdot(12)$.

Die Multiplikation der Substitutionen ist assoziativ: $st\cdot v = s\cdot tv$, so daß die Bezeichnung stv unzweideutig ist. Denn wenn s, t und

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$st = p$ die Substitutionen in (13), (14), (15) bezeichnen und wenn

$$v = \begin{pmatrix} \alpha\beta \dots \lambda \\ A\,B \dots L \end{pmatrix}$$

ist, so ist

$$tv = \begin{pmatrix} a\,b \dots l \\ A\,B \dots L \end{pmatrix}, \quad st \cdot v = pv = \begin{pmatrix} 1\,2 \dots n \\ A\,B \dots L \end{pmatrix} = s \cdot tv.$$

Entsprechend gilt natürlich

$$a \cdot bcd = a[b \cdot cd] = ab \cdot cd = [ab \cdot c]d = abc \cdot d = abcd.$$

Allgemein kann das assoziative Gesetz induktiv bewiesen werden; es zeigt, daß die Bezeichnung $a_1 a_2 \dots a_k$ eindeutig ist. Sind insbesondere alle k Faktoren gleich a, so wird ihr Produkt eindeutig mit a^k bezeichnet und heißt die $k$te Potenz von a.

72. Identische und inverse Substitution. Ordnung einer Substitution. Die Substitution, die jedes Element ungeändert läßt, heißt die identische und wird mit E bezeichnet, da sie mit der Zahl 1 des Zahlensystems vergleichbar ist (denn jede Zahl bleibt bei der Multiplikation mit 1 unverändert).

Eine Substitution p heißt von der Ordnung (oder Periode) k, wenn k die kleinste positive ganze Zahl ist, für welche $p^k = E$. Z. B. haben (12) und (12)(34) beide die Ordnung 2.

Wenn $p = (123 \dots r)$, so wird 1 durch p^2 in 3, durch p^3 in 4, allgemein (für $j < r$) durch p^j in $j + 1$ übergeführt, so daß die Ordnung von p nicht kleiner als r ist. Da außerdem $p^r = E$, so ist die Ordnung eines Zyklus von r Elementen gleich r.

Bilde ich ferner das Produkt $ab \dots$ von zueinander fremden Zyklen (d. h. von Zyklen, die kein Element gemeinsam haben) von $r, s, \dots$ Elementen, so ist $(ab \dots)^k = a^k b^k \dots$ dann und nur dann die Identität E, wenn $a^k = b^k = \dots = E$, d. h. wenn k ein gemeinsames Vielfaches von $r, s, \dots$ ist. Daher ist die Ordnung einer Substitution das kleinste gemeinsame Vielfache der Ordnungen (Elementanzahlen) ihrer Zyklen. Z. B. st (123) (45) von der Ordnung 6, (12) (3456) von der Ordnung 4.

Jede Substitution s besitzt eine inverse s^{-1}, welche die ursprüngliche Substitution wieder rückgängig macht, für die also $s^{-1}s = ss^{-1} = E$. Dies ergibt sich sofort aus

$$(16) \qquad s = \begin{pmatrix} 1\,2 \dots n \\ a\,b \dots l \end{pmatrix}, \quad s^{-1} = \begin{pmatrix} a\,b \dots l \\ 1\,2 \dots n \end{pmatrix}.$$

Übungen: 1. Zeige für $s = (123)$, daß $s^2 = (132)$, $s^3 = E$, $s^{-1} = s^2$ ist. 2. Wenn s die Ordnung k hat, so ist $s^{-1} = s^{k-1}$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

3. Ein Zyklus ändert sich nicht durch eine zyklische Permutation seiner Elemente.

4. Aus $st = sr$ folgt $t = r$.

5. Die Inverse von $(123 \ldots r)$ ist $(r, r-1, \ldots, 2, 1)$.

73. Die Gleichung vierten Grades. Um die Gleichung

$$x^4 + bx^3 + cx^2 + dx + e = 0 \tag{17}$$

zu lösen, bringe man sie auf die Form

$$(x^2 + \tfrac{1}{2}bx)^2 = (\tfrac{1}{4}b^2 - c)x^2 - dx - e.$$

Der Kunstgriff Ferraris (1522—1565) besteht darin, eine Gleichung abzuleiten, in der auch die rechte Seite ein vollständiges Quadrat ist. Dies erreicht man durch Addition von

$$(x^2 + \tfrac{1}{2}bx)y + \tfrac{1}{4}y^2$$

auf beiden Seiten. So erhalten wir

$$(x^2 + \tfrac{1}{2}bx + \tfrac{1}{2}y)^2 = (\tfrac{1}{4}b^2 - c + y)x^2 + (\tfrac{1}{2}by - d)x + \tfrac{1}{4}y^2 - e. \tag{18}$$

Jetzt ist die rechte Seite, die wir kurz mit $q \equiv rx^2 + sx + t$ bezeichnen wollen, dann und nur dann das Quadrat einer linearen Funktion $mx + n$, wenn $s^2 - 4rt = 0$ ist, d. h. — bei Einsetzen der Werte für r, s, t — wenn

$$y^3 - cy^2 + (bd - 4e)y + 4ce - b^2e - d^2 = 0. \tag{19}$$

Hat diese sogenannte kubische Resolvente eine Wurzel y_1, so folgt aus (18), daß

$$x^2 + \tfrac{1}{2}bx + \tfrac{1}{2}y_1 = mx + n \tag{20}$$

oder

$$x^2 + \tfrac{1}{2}bx + \tfrac{1}{2}y_1 = -mx - n.$$

Bezeichnen wir mit x_1, x_2 bzw. x_3, x_4 die Wurzeln dieser beiden Gleichungen, so sind $x_1, \ldots, x_4$ die gesuchten Wurzeln von (17). Man beachte noch, daß

$$x_1x_2 = \tfrac{1}{2}y_1 - n, \quad x_3x_4 = \tfrac{1}{2}y_1 + n, \quad \text{also} \quad x_1x_2 + x_3x_4 = y_1.$$

Geht man statt von y_1 von einer anderen Wurzel y_2 oder y_3 der kubischen Resolvente (19) aus, so erhält man zwei quadratische Gleichungen, deren vier Wurzeln ebenfalls x_1, x_2, x_3, x_4, jedoch in anderer Anordnung als in (20), sind. Die Wurzel, die z. B. jetzt mit x_1 gepaart ist, ist x_3 bzw. x_4. Daher sind die Wurzeln der kubischen Resolvente (19)

$$y_1 = x_1x_2 + x_3x_4, \quad y_2 = x_1x_3 + x_4x_2, \quad y_3 = x_1x_4 + x_2x_3. \tag{21}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Diskriminante von (17) ist wieder definiert als das Produkt der Quadrate ihrer Wurzeldifferenzen. Nun ist nach (21)

$$(22)\qquad \begin{aligned} y_2 - y_3 &= (x_1 - x_2)(x_3 - x_4) \\ y_3 - y_1 &= (x_1 - x_3)(x_4 - x_2) \\ y_1 - y_2 &= (x_1 - x_4)(x_2 - x_3). \end{aligned}$$

Bilden wir das Produkt ihrer Quadrate, so sehen wir, daß die Diskriminante einer biquadratischen Gleichung (17) gleich der Diskriminante ihrer kubischen Resolvente (19) ist.

Übungen: 1. Die kubische Resolvente von $x^4 + 1 = 0$ ist $y^3 - 4y = 0$. Daher hat $x^4 + 1$ die Faktorenpaare $x^2 \pm i$, $x^2 \pm x\sqrt{2} + 1$, $x^2 \pm x\sqrt{-2} - 1$.

2. Die Diskriminante von $x^4 - 8x^3 + 22x^2 - 24x + 9 = 0$ ist Null, so daß die Gleichung eine mehrfache Wurzel hat.

3. Wenn $d = b$, $e = 1$ ist, d. h. wenn eine reziproke Gleichung vorliegt, ist die kubische Resolvente gleich $(y - 2)[y^2 + (2 - c)y + b^2 - 2c] = 0$. Die Tatsache, daß eine ihrer Wurzeln immer gleich 2 ist, folgt unmittelbar aus (21), weil x_1, x_2, x_3, x_4 paarweise reziprok sind. Insbesondere hat $x^4 + x^3 + x^2 + x + 1$ die Faktoren $x^2 + \frac{1}{2}(1 \pm \sqrt{5})x + 1$, wie sich aus der Wahl $y = 2$ ergibt.

74. Substitutionsgruppen. Ein System von m verschiedenen Substitutionen heißt eine Gruppe von der Ordnung m, wenn das Produkt irgend zweier (gleicher oder verschiedener) Elemente des Systems wieder in dem System vorkommt.

Z. B. bilden die $n!$ Substitutionen von n Buchstaben eine Gruppe, da das Produkt zweier Substitutionen wieder eine Substitution ist. Sie heißt die symmetrische Gruppe von n Buchstaben. — Ist ferner s eine Substitution von der Ordnung m, so bilden die Substitutionen $E, s, s^2, \ldots, s^{m-1}$ eine durch s erzeugte (zyklische) Gruppe $m$ter Ordnung.

Eine Gruppe, deren Substitutionen sämtlich in einer anderen Gruppe enthalten sind, heißt eine Untergruppe der letzteren.

Wir wollen sogleich die allgemeine Definition einer Gruppe geben, über deren Elemente keine bestimmten Angaben gemacht sind (die also z. B. keine Substitutionen zu sein brauchen), die vielmehr nur durch gewisse Beziehungen miteinander verknüpft sind. Diese Beziehungen sind:

1. Es ist eine Art der Verknüpfung definiert, welche zwei (gleichen oder verschiedenen) Elementen eindeutig ein drittes Element desselben Systems zuordnet.

2. Für diese Art der Verknüpfung gilt das assoziative Gesetz.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

3. Es gibt ein „Einheitselement", d. h. ein Element E, welches jedes Element a des Systems bei der Verknüpfung ungeändert läßt: $aE = Ea = a$.

4. Es gibt zu jedem Element a ein „inverses" a^{-1} des Systems, welches mit a verknüpft das Einheitselement ergibt:

$$aa^{-1} = a^{-1}a = E.$$

Es ist bezeichnend, daß in dieser Definition weder über die Natur der Elemente noch über die Art der Verknüpfung etwas ausgesagt wird. Trotzdem läßt sich eine ganze Reihe von wichtigen Tatsachen und Sätzen über solche Systeme aufstellen. Und wegen der völlig abstrakten Ausgangsdefinitionen sind diese Sätze in den verschiedensten Teilen der Mathematik anwendbar. —

Es möchte scheinen, als ob wir in unserer Definition der Substitutionsgruppen nur die Bedingung 1 erfüllt hätten. Nach 71. ist aber das assoziative Gesetz von selbst erfüllt. Wenn ferner a eine Substitution $m$ter Ordnung des Systems ist, so ist $a^m = E$, und $a^{m-1} = a^{-1}$ gehört dem System an. Daher folgen auch die Bedingungen (3) und (4).

75. Gruppe, die eine Funktion ungeändert läßt. Wenn $x_1, \ldots, x_4$ voneinander verschieden sind, so sind es auch die drei Funktionen $y_1 = x_1x_2 + x_3x_4$, $y_2 = x_1x_3 + x_4x_2$, $y_3 = x_1x_4 + x_2x_3$. Da nun y_2 und y_3 die einzigen anderen Funktionen derselben Form wie y_1 sind, so kann man ohne nähere Untersuchung schon sagen, daß y_1 durch jede der 24 Substitutionen von $x_1x_2x_3x_4$ in y_1, y_2 oder y_3 übergeführt wird und daher durch $\frac{24}{3} = 8$ Substitutionen ungeändert bleibt. Um dies zu bestätigen, beachte man, daß $a = (12)$ und $b = (13)(24)$ die Funktion $x_1x_2 + x_3x_4$ ungeändert lassen. Dasselbe ist daher für die Produkte

$$c = ab = (1423), \quad d = ba = (1324), \quad e = ca = (14)(23),$$
$$be = (12)(34), \quad a \cdot be = (34)$$

der Fall, d. h. y_1 bleibt bei den 8 Substitutionen des Systems

$$G_8 = \{E, (12), (34), (12)(34), (13)(24), (14)(23), (1423), (1324)\}$$

ungeändert. Offenbar ersetzt aber die Substitution (23) y_1 durch y_2. Dasselbe tun daher auch die 8 Substitutionen, die ich aus denen von G_8 durch Multiplikation mit (23) erhalte. Ebenso ersetzen alle Substitutionen, die ich aus denen von G_8 durch Multiplikation mit (24) erhalte, y_1 durch y_3. Diese drei Systeme von Substitutionen haben, da sie y_1 durch y_1 bzw. y_2 bzw. y_3 ersetzen, kein Element gemeinsam. Daher bilden sie zusammen alle 24 Substitutionen von

Digitized by Google Original from UNIVERSITY OF MICHIGAN

x_1, x_2, x_3, x_4, und daraus schließen wir, daß y_1 durch jede Substitution der x in y_1, y_2, y_3 übergeführt wird, so daß y_1 eine dreiwertige Funktion ist. Ferner schließen wir, daß G_8 aus allen Substitutionen der x besteht, die y_1 ungeändert lassen. Daher ist jedes Produkt zweier Substitutionen von G_8 wieder eine Substitution von G_8, d. h. G_8 ist eine Gruppe von der Ordnung 8.

Wir sagen, die Funktion $x_1x_2 + x_3x_4$ **gehört** zu der Gruppe G_8, da sie durch alle Substitutionen von G_8 ungeändert bleibt, während sie durch alle anderen Substitutionen von x_1, x_2, x_3, x_4 ihren Wert ändert.

Ferner sahen wir, daß man die 8 Substitutionen von G_8 durch sukzessive Multiplikation von a und b erhält; a und b heißen daher die „Erzeugenden" von G_8.

Übungen: 1. Da $y_2 = x_1x_3 + x_4x_2$ aus y_1 durch Vertauschung von x_2 und x_3 hervorgeht, so bekommt man die zu y_2 gehörende Gruppe H_8, indem man 2 und 3 in G_8 vertauscht:

$$H_8 = \{E, (13), (24), (13)(24), (12)(34), (14)(23), (1432), (1234)\}.$$

2. Ebenso erhält man durch Vertauschung von 2 und 4 aus G_8 die Gruppe

$$K_8 = \{E, (14), (23), (14)(23), (13)(24), (12)(34), (1243), (1342)\},$$

welche zu $y_3 = x_1x_4 + x_2x_3$ gehört. Die zwei Erzeugenden dieser Gruppe sind (14) und (13)(24).

3. Für $t = x_1 + x_2 - x_3 - x_4$ ist $t^2 = 4y_1 + b^2 - 4c$. Daher läßt eine Substitution, die t ungeändert läßt, auch y_1 ungeändert. Man zeige, daß t zu der Untergruppe $\{E, (12), (34), (12)(34)\}$ von G_8 gehört.

4. Die sechs Funktionen, die man aus $\varphi = y_1 + \omega y_2 + \omega^2 y_3$ durch Permutation der y bekommt, sind alle voneinander verschieden, wenn $x_1, \ldots, x_4$ unabhängige Variabeln sind. Daher gehört φ zu der Gruppe G, die aus den Substitutionen der x besteht, welche y_1, y_2, y_3 gleichzeitig ungeändert lassen, d. h. G ist die größte gemeinsame Untergruppe, der sog. Durchschnitt, von G_8, H_8, K_8, also

$$G = \{E, (12)(34), (13)(24), (14)(23)\}.$$

Man weise nach, daß G eine kommutative Gruppe ist, d. h. daß für beliebige Elemente a und b die Beziehung gilt: $ab = ba$.

5. Für drei voneinander verschiedene Werte der x gehört

$$(x_2 - x_3)(x_3 - x_1)(x_1 - x_2)$$

zu der zyklischen Gruppe $\{E, (123), (132)\}$, deren Erzeugende (123) ist.

76. Die alternierende Gruppe. Eine Transposition ist eine Substitution, welche zwei Buchstaben miteinander vertauscht und die anderen ungeändert läßt, z. B. (13). Jede Substitution ist ein Produkt von Transpositionen. Denn sie ist ein Produkt von Zyklen,

Digitized by Google Original from UNIVERSITY OF MICHIGAN

die kein Element gemeinsam haben, und jeder Zyklus ist ein Produkt von Transpositionen:

$$(123 \ldots n-1, n) = (12)(13) \ldots (1, n-1)(1, n).$$

Jedoch läßt sich ein und dieselbe Substitution auf verschiedene Weisen in Transpositionen zerlegen; z. B.

$$(123) = (12)(13) = (13)(23) = (13)(23) \cdot (45)(45).$$

Indessen bestehen die verschiedenen Zerlegungen einer gegebenen Substitution s in Transpositionen entweder alle aus einer graden Zahl von Transpositionen — dann heißt s eine grade oder positive Substitution — oder alle aus einer ungraden Zahl von Transpositionen — dann heißt s eine ungrade oder negative Substitution. Die alternierende Funktion

$$\begin{aligned} P = {} & (x_1 - x_2)(x_1 - x_3)(x_1 - x_4), \ldots, (x_1 - x_n) \\ & \cdot (x_2 - x_3)(x_2 - x_1), \ldots, (x_2 - x_n) \\ & \cdot \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\ & \cdot (x_{n-1} - x_n) \end{aligned}$$

ändert nämlich durch jede Transposition $(x_i x_j)$ lediglich ihr Vorzeichen (vgl. 75., Übung 5); denn die Faktoren von P, die weder x_i noch x_j enthalten, bleiben ungeändert; der Faktor $x_i - x_j$ ändert sein Zeichen, und die übrigen Faktoren können paarweise zu Produkten der Form

$$(x_i - x_k)(x_j - x_k), \quad \text{wo} \quad k = 1, 2, \ldots, n; \ k \neq i; \ k \neq j,$$

zusammengefaßt werden. Jedes solche Produkt ändert sich aber nicht. Daher ändert P nur sein Vorzeichen.

Ist nun s das Produkt einer graden Zahl von Transpositionen, so bleibt P ungeändert, im anderen Fall geht es in $-P$ über. Da eine Substitution entweder P ungeändert läßt oder in $-P$ überführt, so ist jede Substitution entweder stets aus einer graden oder stets ungraden Zahl von Transpositionen zusammensetzbar.

Alle graden Substitutionen von n Buchstaben bilden daher eine Gruppe, die sog. alternierende Gruppe von n Buchstaben. Zu ihr gehört die alternierende Funktion P.

77. Satz: Wenn eine Gruppe G eine ungrade Substitution t enthält, so ist genau die Hälfte aller Substitutionen von G ungrade.

G muß mindestens eine grade Substitution enthalten, weil ja das Produkt zweier ungraden Substitutionen grade ist, andererseits aber in G liegen muß. Multipliziert man alle graden Substitutionen von G mit t, so sind diese Produkte voneinander verschieden und ungrade, so daß G mindestens so viel ungrade Substitutionen wie grade enthält. Andererseits sind die Produkte von t

Digitized by Google Original from UNIVERSITY OF MICHIGAN

mit allen ungraden Substitutionen von G grade, so daß G mindestens so viel grade Substitutionen wie ungrade enthält. Daraus folgt der Satz. — Er zeigt, daß die alternierende Gruppe von n Buchstaben die Ordnung $\frac{1}{2}n!$ besitzt. Da sie eine Untergruppe der symmetrischen Gruppe ist, so haben wir ein Beispiel für den nächsten Satz.

78. Satz: Die Ordnung einer Untergruppe ist ein Teiler der Ordnung der ganzen Gruppe.

G sei eine Gruppe $r$ter Ordnung, H eine Untergruppe von der Ordnung $s < r$, so daß G mindestens eine Substitution, etwa g_2, enthält, die nicht in H vorkommt. Multipliziert man jede Substitution von H mit g_2 und bezeichnet diesen Komplex von Substitutionen kurz mit Hg_2, so kann keine Substitution hg_2 von Hg_2 gleich einer Substitution h' von H sein, denn sonst wäre $g_2 = h^{-1}h'$ ein Element der Gruppe H, gegen die Voraussetzung. Daher enthält der Komplex $H + Hg_2$ $2s$ verschiedene Substitutionen. Ist nun $r = 2s$, so ist unser Satz bewiesen. Andernfalls enthält G noch eine Substitution g_3, die weder in H noch in Hg_2 vorkommt. Wie oben gehört keine Substitution von Hg_3 zu H. Wenn andererseits eine Substitution hg_3 von Hg_3 gleich der Substitution $h'g_2$ von Hg_2 wäre, so wäre $g_3 = h^{-1}h'g_2 = h_1g_2$ ein Element von Hg_2, gegen die Voraussetzung. Daher enthält der Komplex $H + Hg_2 + Hg_3$ $3s$ verschiedene Substitutionen. Da die Ordnung von G kleiner als oder gleich $n!$ sein muß, so muß das Verfahren notwendig zu einem Ende führen und ergibt

$$G = H + Hg_2 + Hg_3 + \cdots + Hg_u.$$

Daher ist $r = su$. Die Zahl u heißt der Index von H unter G.

Übungen: 1. Die Ordnung jeder Gruppe von n Elementen ist ein Teiler von $n!$

2. Die Ordnung jeder Substitution von G ist ein Teiler der Ordnung von G. (Denn jede Substitution erzeugt eine Untergruppe von derselben Ordnung.)

3. Eine Gruppe von Primzahlordnung ist daher zyklisch. (Denn sie kann keine eigentliche Untergruppe enthalten, so daß sie durch jedes ihrer Elemente mit Ausnahme von E erzeugt wird.)

4. Die alternierende Gruppe von 4 Elementen besteht aus

$$E,\ (12)(34),\ (13)(24),\ (14)(23)$$

und den 8 Zyklen von 3 Buchstaben.

5. Die in zwei Gruppen gleichzeitig enthaltenen Substitutionen, der sog. „Durchschnitt", bilden eine Untergruppe von jeder der beiden Gruppen. Denn mit a und b ist auch ab in beiden Gruppen enthalten.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

NEUNTES KAPITEL.

KÖRPER.

REDUZIBLE UND IRREDUZIBLE FUNKTIONEN.

Dieses Kapitel enthält einige Begriffe und elementare Sätze, die in der Galoisschen Theorie der Gleichungen gebraucht werden.

79. Körper. Adjunktion. Ein System komplexer Zahlen heißt ein Zahlkörper, wenn Summe, Differenz, Produkt und Quotient (die Division durch Null wird dabei natürlich ausgeschlossen) irgend zweier (gleicher oder verschiedener) Zahlen des Systems wieder dem System angehört. — Beispiele hatten wir in 28. schon gegeben.

Alle rationalen Funktionen einer oder mehrerer Variablen mit Koeffizienten aus einem Zahlkörper bilden einen Funktionenkörper. In der Galoisschen Theorie der Gleichungen verwendet man einen Körper $R(K_1, \ldots, K_m)$, der aus allen rationalen Funktionen von $K_1, \ldots, K_m$ mit rationalen Koeffizienten besteht. Dabei können die Koeffizienten Konstanten sein oder gegebene Funktionen genau angegebener Variablen, die nicht notwendigerweise unabhängig zu sein brauchen. Z. B. besteht $R(\sqrt{3})$ aus allen Zahlen

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}},$$

wo a, b, c, d rationale Zahlen und c und d nicht beide gleich Null sind. Durch Rationalmachen des Nenners bekommt man die Form $e+f\sqrt{3}$, wo e und f rational sind. Daher besteht $R(\sqrt{3}, x)$ aus allen rationalen Funktionen von x, deren Koeffizienten die Form $e+f\sqrt{3}$ haben.

Die Elemente (Zahlen oder Funktionen) eines Körpers heißen allgemein Größen.

Obgleich das System, das nur aus der Zahl Null besteht, auch der obigen Definition genügt, setzen wir doch fest, daß jeder Körper K mindestens eine von Null verschiedene Größe q enthält. Daher enthält er auch $\frac{q}{q} = 1$, $1+1=2$ usw. und daher auch alle

Digitized by Google Original from UNIVERSITY OF MICHIGAN

rationalen Zahlen. Mit anderen Worten: Der Körper R aller rationaler Zahlen ist ein Unterkörper jedes Körpers K. Der oben erwähnte Körper $R(K_1, \ldots, K_m)$ entsteht aus R durch „Adjunktion" von $K_1, \ldots, K_m$ zu R. Ist $n < m$, so entsteht $R(K_1, \ldots, K_m)$ aus $R(K_1, \ldots, K_n)$ durch Adjunktion von $K_{n+1}, \ldots, K_m$.

Übungen: 1. Jede Zahl von $R(i)$, wo $i^2 = -1$, kann in die Form $e + fi$ gebracht werden, wo e und f rational sind.

2. $R(\sqrt{3}) = R(\sqrt{12})$.

3. Setzt man $r = i\sqrt{3}$, $\omega = -\frac{1}{2} + \frac{1}{2}r$, so ist $R(r) = R(\omega) = R(\omega^2)$.

4. Es ist $R(i, \sqrt{2}) = R(i + \sqrt{2})$.

Anleitung: $R(i - \sqrt{2}) = R\left(-\frac{3}{i + \sqrt{2}}\right) = R(i + \sqrt{2})$.

5. Nach Beispiel 4 entsteht $R(i + \sqrt{2})$ aus $R(i)$ durch Adjunktion von $\sqrt{2}$.

80. Der größte gemeinsame Teiler. $f(x)$ und $g(x)$ seien Polynome in x mit Koeffizienten aus K, und $g(x)$ sei nicht identisch Null. Die Division von $f(x)$ durch $g(x)$ ergebe als Quotient $a(x)$ und als Rest $r(x)$, dessen Grad natürlich geringer ist als der von $g(x)$. Ähnlich ergebe die Division von g durch r den Quotienten b und den Rest s, dessen Grad in x geringer ist als der von r. Fährt man so fort, so möge man

$$f = ga + r, \quad g = rb + s, \quad r = sc + t, \quad s = td$$

erhalten, so daß wir also bei dem vierten Rest stehen geblieben sind und ihn gleich Null gesetzt haben. Da $a, r, b, \ldots$ durch rationale Operationen erhalten werden, so sind alle ihre Koeffizienten Größen in K.

Jeder gemeinsame Teiler von f und g ist auch ein Teiler von r, s, t. Geht man die Gleichungen in umgekehrter Reihenfolge durch, so sieht man, daß t ein Teiler von s, r, g und f ist. Da also t ein Teiler von f und g ist und da umgekehrt jeder gemeinsame Teiler der letzteren ein Teiler von t ist, so ist t der größte gemeinsame Teiler von f und g. Er ist (bis auf einen zu K gehörigen Faktor) eindeutig bestimmt. Insbesondere gibt es einen einzigen größten gemeinsamen Teiler, der als Koeffizienten der höchsten Potenz von x die Zahl 1 hat.

Die erwähnten Gleichungen geben der Reihe nach

$$r = f - ga, \quad s = g(1 + ab) - fb,$$
$$t = f(1 + bc) - g(a + c + abc).$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Aus ihnen und dem Vorhergehenden ergibt sich

Satz 1: *Zwei Polynome $f(x)$ und $g(x)$, die nicht beide identisch verschwinden und deren Koeffizienten einem Körper K angehören, haben einen einzigen gemeinsamen größten Teiler (kurz: g. g. T.) $d(x)$, dessen Leitkoeffizient gleich 1 ist. Alle seine Koeffizienten gehören zu K, und es gibt zwei Polynome $u(x)$, $v(x)$ mit Koeffizienten aus K, so daß*

$$d(x) \equiv u(x)f(x) + v(x)g(x).$$

Die obige Untersuchung ist auch im Falle, daß f und g ganze Zahlen sind, anwendbar. Ist der g. g. T. gleich 1, so heißen f und g relativ prim oder teilerfremd. So haben wir

Satz 2: Wenn f und g teilerfremd sind, so gibt es zwei ganze Zahlen u und v derart, daß $uf + vg = 1$.

81. Wurzeln algebraischer Gleichungen. Betrachten wir eine algebraische Gleichung

$$f(x) \equiv x^n + c_1 x^{n-1} + \cdots + c_n = 0. \tag{1}$$

Für $n = 3$ oder 4 fanden wir in Kap. VII Formeln, welche die n Wurzeln von (1) durch die c_i ausdrücken. Für $n > 4$ gibt es indessen keine solchen Formeln, abgesehen von speziellen Gleichungen wie $x^n - c = 0$.

Was versteht man nun unter den Wurzeln von (1), wenn die Koeffizienten c_i unabhängige Variabeln sind? In diesem Fall führt die Methode von 80. zum Aufsuchen des größten gemeinsamen Teilers von $f(x)$ und seiner Ableitung $f'(x)$ schließlich zu einem Rest $r(c_1, \ldots, c_k)$, der von x frei ist und nicht identisch verschwindet. (So ist z. B. für

$$f(x) \equiv x^n - 1, \quad f'(x) = nx^{n-1} \quad \text{und} \quad r = -1.)$$

Es seien also $C_1, \ldots, C_n$ solche konstanten Werte von $c_1, \ldots, c_n$, daß $r(C_1, \ldots, C_n) \neq 0$. Dann hat die zugehörige Funktion (1) keinen Faktor mit ihrer Ableitung gemeinsam, und die Gleichung (1) hat n verschiedene Wurzeln. Da r als Polynom eine stetige Funktion der c ist, so ist auch $r(c_1, \ldots, c_n) \neq 0$ für alle Wertsysteme der c, für welche die Differenzen $c_i - C_i$ ihrem absoluten Werte nach hinreichend klein sind. Für jedes solche Wertsystem der c hat Gleichung (1) n verschiedene Wurzeln $X_1, \ldots, X_n$, und jede Wurzel X_i ändert sich bekanntlich[1]) stetig, wenn sich die c stetig

1) Webers Lehrbuch der Algebra I, 2. Ausg., 1898, p. 148. Vgl. Coolidge, Annals of Mathem. (2), 9, 1908, pp. 116—118.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ändern, d. h. die X_i sind stetige Funktionen x_i der $c_1, \ldots, c_n$ für solche Werte der c, für die $|c_i - C_i|$ hinreichend klein ist. Diese Funktionen $x_1, \ldots, x_n$ heißen die Wurzeln von (1).

Wenn die c_i keine unabhängigen Variabeln, sondern Funktionen von gewissen Variabeln v_j sind von der Art, daß $r(c_1, \ldots, c_n)$ in den v_j nicht identisch verschwindet, so bleibt obige Überlegung bestehen, wenn wir jetzt nur solche Werte der $c_1, \ldots, c_n$ betrachten, die man durch stetige Abänderung der v_j bekommt.

82. Reduzibilität. Ein Polynom in einer Variabeln x mit Koeffizienten aus einem Körper K[1]) heißt in K reduzibel, wenn es sich als Produkt von Polynomen in x (die sich nicht auf Konstanten reduzieren dürfen) mit Koeffizienten aus K darstellen läßt. Ist eine Zerlegung in solche Faktoren nicht möglich, so heißt es irreduzibel in K.

Z. B. ist im Körper R der rationalen Zahlen $x^2 - 4$ reduzibel und $x^2 - 2$ irreduzibel. Hingegen ist $x^2 - 2$ in $R(\sqrt{2})$ reduzibel.

Je nachdem $f(x)$ in K reduzibel ist oder nicht, heißt auch die Gleichung $f(x) = 0$ reduzibel bzw. irreduzibel in K.

Satz 3: Sind $f(x)$ und $g(x)$ zwei Polynome in K und ist $f(x)$ in K irreduzibel, so ist, wenn $f(x) = 0$ und $g(x) = 0$ eine Wurzel gemeinsam haben, $f(x)$ ein Teiler von $g(x)$.

Der g. g. T. $d(x)$ von $f(x)$ und $g(x)$ reduziert sich nicht auf eine Konstante, sondern hat mindestens den Faktor $x - a$. Nach 80. gehören die Koeffizienten von $d(x)$ zu K. Nun ist der Quotient von $f(x)$ und $d(x)$ eine Konstante, weil sonst $f(x)$ in K reduzibel wäre, d. h. es ist $f(x) \equiv c \cdot d(x)$, wo c eine von x unabhängige Größe aus K ist. Da nun $d(x)$ in $g(x)$ aufgeht, so geht auch $f(x)$ in $g(x)$ auf.

Übungen: 1. Die Wurzel einer in K irreduziblen Gleichung genügt keiner Gleichung in K von niedrigerem Grade.

Denn sonst wäre diese niedere Gleichung ein Teiler der anderen.

2. Eine irreduzible Gleichung hat keine mehrfachen Wurzeln.

Denn sonst hätte sie mit ihrer Ableitung eine gemeinsame Wurzel.

3. Zwei in K irreduzible Gleichungen sind identisch, wenn sie eine gemeinsame Wurzel haben.

4. $x^4 + 1$ ist in jedem Körper reduzibel, welcher eine der Zahlen $\sqrt{2}$, $\sqrt{-2}$, $i = \sqrt{-1}$, $\varrho = \frac{1}{2}(1 + i)\sqrt{2}$ enthält, jedoch in jedem anderen Körper irreduzibel.

---

1) Kurz: ein Polynom in K oder aus K.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Denn seine lineare Faktoren sind $x \pm \varrho, x \pm \varrho^{-1}$, seine quadratischen $x^2 \pm i$, $x^2 \pm x\sqrt{2} + 1$, $x^2 \pm x\sqrt{-2} - 1$.

83. Das Gaußsche Lemma. Wenn ein normiertes[1]) Polynom $f(x)$ mit ganzen Koeffizienten in zwei Polynome

$$\varphi(x) = x^m + b_1 x^{m-1} + \cdots + b_m$$
$$\psi(x) = x^n + c_1 x^{n-1} + \cdots + c_n$$

mit rationalen Koeffizienten zerlegbar ist, so sind diese Koeffizienten ganze Zahlen.

Zum Beweise bringe man die Brüche $b_1, \ldots, b_m$ auf ihren gemeinsamen (kleinsten) Nenner B_0, so daß $b_i = \frac{B_i}{B_0}$. Dann sind $B_0, \ldots, B_m$ ganze Zahlen ohne gemeinsamen Teiler. — Ähnlich ist $c_i = \frac{C_i}{C_0}$, wo auch die C ganze teilerfremde Zahlen sind. Dann ist der Satz offenbar schon bewiesen, wenn $B_0 = C_0 = 1$ ist. Man nehme daher $B_0 C_0 > 1$ an. Multipliziert man die Identität $f \equiv \varphi\psi$ mit $B_0 C_0$, so erhält man

$$B_0 C_0 \cdot f(x) \equiv gh, \tag{2}$$

wo
$$g = B_0 x^m + B_1 x^{m-1} + \cdots + B_m,$$
$$h = C_0 x^n + C_1 x^{n-1} + \cdots + C_n.$$

Es sei nunmehr p ein Primfaktor von $B_0 C_0$. Da p jeden Koeffizienten auf der linken Seite von (2) teilt, so teilt es auch jeden Koeffizienten von gh. Nun können aber nicht alle Koeffizienten von g durch p teilbar sein, da die B teilerfremd sind. B_i sei daher der erste Koeffizient in g, der durch p nicht teilbar ist. Ebenso sei C_k der erste solche Koeffizient in h. Der Gesamtkoeffizient von $x^{m+n-i-k}$ in gh ist nun

$$\cdots + B_{i+2}C_{k-2} + B_{i+1}C_{k-1} + B_i C_k + B_{i-1}C_{k+1} + B_{i-2}C_{k+2} + \cdots$$

Da aber $B_{i-1}, B_{i-2}, \ldots, B_0$ und $C_{k-1}, C_{k-2}, \ldots, C_0$ alle den Teiler p haben, $B_i C_k$ jedoch nicht, so ist die vorstehende Summe nicht durch p teilbar, entgegen dem oben Gesagten.

Übungen: 1. Das Gaußsche Lemma zeigt für $m = 1$, daß, wenn eine normierte Gleichung $x^r + a_1 x^{r-1} + \cdots + a_r = 0$ mit ganzen Koeffizienten eine rationale Wurzel hat, diese Wurzel ganzzahlig ist.

1) D. h. ein Polynom, in dem der Koeffizient der höchsten Potenz von x gleich 1 ist.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

2. Eine ganzzahlige Wurzel der Gleichung in Beispiel 1 ist ein Teiler des absoluten Gliedes a_r.

Denn sie teilt alle Glieder mit Ausnahme des letzten.

3. Man zeige, daß $x^3 - 2$, $x^3 - 3x + 1$, $x^3 - 7x + 7$ im Körper R der rationalen Zahlen irreduzibel sind. — Anleitung: Wenn eine dieser Funktionen in R reduzibel wäre, so wäre sie das Produkt einer linearen und einer quadratischen Funktion in R. Jetzt wende man die Sätze von Beispiel 1 und 2 an.

84. Die Irreduziblität von $x^p - A$.

Satz 4: Wenn p eine Primzahl ist und A eine Größe aus K, die nicht die $p$te Potenz einer anderen Größe aus K ist, so ist $x^p - A$ in K irreduzibel.

Eine imaginäre $p$te Einheitswurzel hat die Form

$$\varrho = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p},$$

und zwar ist nach dem Moivreschen Satz $\varrho^m \neq 1$, wenn $0 < m < p$. Daher sind $1, \varrho, \varrho^2, \ldots, \varrho^{p-1}$ alle voneinander verschieden, denn wenn etwa $\varrho^i = \varrho^k$ wäre, so wäre $\varrho^{i-k} = 1$, wo $i - k < p$. Die Potenzen $1, \varrho, \varrho^2, \ldots, \varrho^{p-1}$ liefern daher alle $p$ten Einheitswurzeln. Ist also r eine der Wurzeln von $x^p = A$, so liefert das System

$$r, \varrho r, \varrho^2 r, \ldots, \varrho^{p-1} r \tag{3}$$

alle Wurzeln der Gleichung. Angenommen nun, $x^p - A$ habe den normierten Faktor $f(x)$ in K vom Grade $t < p$. Dann wäre das Produkt $\varrho^s r^t$ aller Wurzeln von $f(x) = 0$, da es (abgesehen vom Vorzeichen) gleich dem absoluten Gliede ist, eine Zahl aus K, und nach Satz 2 gäbe es dann ganze Zahlen y und z, für die $ty - pz = 1$ wäre. Nun wäre aber mit $\varrho^s r^t$ auch

$$(\varrho^s r^t)^y = \varrho^{sy} r^{py-z+1} = \varrho^{sy} r A^z = r' A^z,$$

wo r' eine der Wurzeln (3) ist, in K enthalten. Da aber A^z eine Zahl aus K ist, so wäre auch r' eine solche Zahl, d. h. A wäre die $p$te Potenz einer Größe r' aus K, gegen unsere Voraussetzung. Daher ist $x^p - A$ in K irreduzibel (vgl. 83., Beisp. 3).

85. Irreduzibilität der Kreisteilungsgleichung. Wenn p eine Primzahl ist, so hat die Gleichung

$$\frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$$

als Wurzeln die imaginären $p$ten Einheitswurzeln.

Allgemein hat

$$f(x) \equiv \frac{x^{tp} - 1}{x^t - 1} \equiv x^{t(p-1)} + x^{t(p-2)} + \cdots + x^t + 1 \quad \text{für} \quad t = p^{s-1}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

als Wurzeln die primitiven p^sten Einheitswurzeln, d. h. diejenigen Wurzeln von $x^{p^s} = 1$, die nicht schon einer ähnlichen Gleichung niedrigeren Grades (in diesem Falle $x^t = 1$) genügen.

Bezeichnet ϱ eine beliebige der primitiven p^sten Einheitswurzeln, so ist die Gesamtheit der t Wurzeln von $x^t = 1$ gegeben durch das System $\varrho^p, \varrho^{2p}, \ldots, \varrho^{tp} = 1$. Die $e = tp - t$ übrigen Potenzen von ϱ mit positiven Exponenten $a_1, a_2, \ldots, a_e$, die kleiner als tp und nicht teilbar durch p sind, liefern die Gesamtheit der Wurzeln von $f(x) = 0$.

Ist z. B. $p^s = 9$, so geben $\varrho^3, \varrho^6, \varrho^9$ die Wurzeln von $x^3 = 1$, während $\varrho, \varrho^2, \varrho^4, \varrho^5, \varrho^7, \varrho^9$ die Wurzeln von $x^6 + x^3 + 1 = 0$, d. h. die primitiven neunten Einheitswurzeln sind.

Nehmen wir jetzt an, $f(x)$ sei im Körper R der rationalen Zahlen reduzibel (kurz: R reduzibel). Dann zerfällt $f(x)$ nach dem Gaußschen Lemma in $\varphi(x)$ und $\psi(x)$ mit bekannten Eigenschaften. Wegen $f(1) = p$ ist $p = \varphi(1) \cdot \psi(1)$, und, da p eine Primzahl ist, muß eine dieser Zahlen, etwa $\varphi(1)$, den Wert ± 1 haben. Nun ist mindestens eine der Wurzeln $\varrho^{a_1}, \ldots, \varrho^{a_e}$ von $f(x) = 0$ eine Wurzel von $\varphi(x) = 0$, so daß

$$\varphi(\varrho^{a_1}) \cdot \varphi(\varrho^{a_2}) \ldots \varphi(\varrho^{a_e}) = 0.$$

Dies zeigt, daß die Funktion

$$P(x) \equiv \varphi(x^{a_1}) \cdot \varphi(x^{a_2}) \ldots \varphi(x^{a_e})$$

verschwindet, wenn x durch irgendeine der Wurzeln ϱ von $f(x) = 0$ (welches ja keine mehrfache Wurzel hat) ersetzt wird; es ist daher

$$P(x) \equiv f(x) \cdot q(x),$$

wo das Polynom $q(x)$ nach dem Gaußschen Lemma ganze Koeffizienten hat. Setzt man $x = 1$ und erinnert sich, daß $f(1) = p$, so bekommen wir

$$P(1) = (\varphi(1))^e = (\pm 1)^e = f(1) \cdot q(1) = p \cdot q(1),$$

wo q eine ganze Zahl ist. Da dies unmöglich ist, so haben wir den

Satz 5: Ist p eine Primzahl, so ist die Kreisteilungsgleichung $f(x) = 0$, deren Wurzeln die primitiven p^sten Einheitswurzeln sind, in R irreduzibel.

Übungen: 1. Für $p^s = 3$ ist $f(x) = x^2 + x + 1$, für $p^s = 2^2$ ist $f(x) = x^2 + 1$. Man bestätige, daß diese quadratischen Funktionen in R irreduzibel sind.

2. Für $p^s = 5$ ist $f(x) = x^4 + x^3 + x^2 + x + 1$. Man bestätige die Irreduzibilität in R, indem man annimmt, daß $f(x) \equiv (x^2 + a x \pm 1)(x^2 + b x \pm 1)$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ZEHNTES KAPITEL.

DIE GRUPPE EINER GLEICHUNG FÜR EINEN GEGEBENEN KÖRPER.

86. Einleitung. Mit einer gegebenen algebraischen Gleichung ist eine gewisse Substitutionsgruppe G ihrer Wurzeln verbunden. Der Begründer dieser Theorie ist E. Galois, der 1832 im Alter von 21 Jahren im Duell fiel; seine Abhandlung über Gleichungstheorie wurde nach seinem Tode von Liouville herausgegeben.[1]) — In einem späteren Kapitel werden wir zeigen, daß eine Gleichung durch Radikale lösbar ist, wenn ihre Gruppe „auflösbar" ist, und umgekehrt, und wir werden daraus schließen, daß die allgemeine Gleichung vom fünften und höheren Grade nicht durch Radikale lösbar ist. — In einem weiteren Kapitel werden wir dann unsere Theorie auf eine Reihe von Fragen anwenden, die über die elementare Geometrie hinausgehen, und z. B. die Unmöglichkeit der Dreiteilung des Winkels mit Zirkel und Lineal beweisen.

87. Gleiche Funktionen der Wurzeln. Wir gehen von der Gleichung

$$f(x) \equiv x^n + c_1 x^{n-1} + \cdots + c_n = 0 \tag{1}$$

aus, deren Koeffizienten Funktionen gewisser Variablen v_j sind. Wir haben in 81. auseinandergesetzt, was man unter den n Wurzeln von (1), welche Funktionen der v_j sind, versteht.

Zwei Polynome φ und ψ in den Wurzeln $x_1, \ldots, x_n$ heißen gleich, wenn sie für alle Wertsysteme von $c_1, \ldots, c_n$ (von denen ja die Wurzeln abhängen) dieselben Werte annehmen. Falls φ und ψ rationale Funktionen der x_i sind, legen wir den c_i die weitere Beschränkung auf, daß die Nenner von φ und ψ von Null verschieden sind.

Sind φ und ψ nicht gleich, so heißen sie verschieden.

---

1) Journ. de Math. 11, 1846, pp. 381—444; Œuvres 1897; Manuscrits de Galois 1908. — Über Galois Leben vgl. Bull. Amer. Math. Soc. 4, 1897/98, p. 332; Scientific Monthly, 1921, pp. 363—375.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Nehmen wir z. B. die reziproke Gleichung

$$x^4 + ax^3 + bx^2 + ax + 1 = 0, \tag{2}$$

wo a und b unabhängige komplexe Variablen sind. Da der reziproke Wert einer Wurzel wieder eine Wurzel ist, können wir die Bezeichnung der Wurzeln so wählen, daß für alle a und b $x_1x_2 = 1$, $x_3x_4 = 1$. Daher sind die beiden Funktionen x_1x_2 und x_3x_4 gleich und ebenso die Funktionen $\frac{x_1}{x_3}$ und $\frac{x_2}{x_4}$. — Ferner haben wir für $t = x_1 + x_2 - x_3 - x_4$ und $y_1 = x_1x_2 + x_3x_4$

$$t^2 = (\sum x_1)^2 - 4\sum x_1x_2 + 4y_1,$$

d. h. die Funktionen t^2 und $a^2 - 4b + 4y_1$ sind gleich.

Wenn man die Funktion ψ aus φ durch Anwendung einer Substitution s auf $x_1, \ldots, x_n$ bekommt und wenn φ und ψ in obigem Sinne gleich sind, so sagt man, daß φ durch die Substitution s ungeändert bleibt oder daß es sie erträgt oder daß es sich ihr gegenüber invariant verhält.

Bei (2) bleibt x_1x_2 durch die beiden Substitutionen (13) (24) und (1324) ungeändert, jedoch nicht durch (13).

88. $n!$ wertige Funktionen der n Wurzeln. Wir können, ohne daß unser Studium einer Gleichung $f(x) = 0$ an Allgemeinheit verliert, die n Wurzeln von $f(x) = 0$ als verschieden voraussetzen. Denn im anderen Fall hätten $f(x)$ und $f'(x)$ den g. g. T. $g(x)$ und $f(x):g(x) = 0$ besäße alle Wurzeln von $f(x)$, aber jede nur ein einziges Mal. Wir setzen daher immer die Wurzeln $x_1, \ldots, x_n$ von $f(x) = 0$ alle als verschieden voraus. Dann gilt der

Satz 1: Es gibt ganze Zahlen $m_1, \ldots, m_n$ von der Beschaffenheit, daß aus

$$V_1 = m_1x_1 + m_2x_2 + \cdots + m_nx_n \tag{3}$$

$n!$ verschiedene Funktionen V_s hervorgehen, wenn man auf die $x_1, \ldots, x_n$ alle die $n!$ Substitutionen s ausübt.

Für $n = 2$ setzen wir $m_1 = 1$, $m_2 = 0$, also $V_1 = x_1$. — Der Fall $n = 3$ wurde in 69., Beispiel 5 behandelt.

Man bilde zum Beweise alle $p = n!\,(n! - 1)$ zwischen den V möglichen Differenzen $V_s - V_t$ (wo $s \neq t$) und multipliziere sie alle miteinander. Dann bekommt man eine Form in den m, die sich jetzt durch Permutation der x nicht mehr ändert, deren Koeffizienten also symmetrische Funktionen der x und also auch Funktionen der Koeffizienten von $f(x)$ sind. Diese Form hat in den m den Grad p, und man kann offenbar solche ganzen Zahlen für

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$m_1, \ldots, m_n$ auswählen, daß die Form $\neq 0$ wird. Denn für $n-1$ der m kann man ganz beliebige ganzzahlige Werte annehmen (wenn nur das entstandene Polynom nichtidentisch verschwindet), das letzte m muß dann so gewählt werden, daß das Polynom $p$ten Grades in diesem m von Null verschieden ist; das ist aber immer möglich, da es ja höchstens p ganzzahlige Werte von m gibt, welche zu vermeiden sind.

Übungen: 1. Die Wurzeln von $x^3+x^2+x+1=0$ sind $x_1=-1$, $x_2=i$, $x_3=-i$. Man zeige, daß $x_2+m_3x_3$ sechswertig ist, wenn m_3 von $0, 1, \pm i, 1\pm i, \frac{1}{2}(1\pm i)$ verschieden, also z. B. gleich -1 ist. Ebenso ist auch x_2-x_1 sechswertig.

Man bezeichne die 6 Substitutionen von x_1, x_2, x_3 mit

$$E,\ a=(12),\ b=(13),\ c=(23),\ d=(123),\ e=(132).$$

Man berechne die folgenden Funktionen und bestätige, daß sie verschieden sind:

$$V_1=x_2-x_1=1+i, \qquad V_b=x_2-x_3=2i, \qquad V_c=x_3-x_1=1-i,$$
$$V_a=-V_1, \qquad V_d=-V_b, \qquad V_e=-V_c.$$

2. Ebenso ist die Funktion (3) $n!$wertig, wenn die x_i unabhängige Variablen und $m_1, \ldots, m_n$ irgendwelche voneinander verschiedene Konstanten sind.

89. Galoissche Resolventen. Die Substitutionen von $x_1, \ldots, x_n$ bezeichne man mit $s_1, \ldots, s_r$, wo s_1 die identische Substitution und $r=n!$ ist. V_1 sei die $r$wertige Funktion (3). Transformieren wir V_1 durch s_j und die resultierende Funktion V_{s_j} durch s_k, so erhalten wir V_{s_l}, wo $s_l=s_js_k$. Läßt man j bei festem k die Werte $1, \ldots, r$ durchlaufen, so durchläuft l dieselben Werte $1, \ldots, r$ in anderer Anordnung. Daher werden $V_1, \ldots, V_{s_r}$ durch s_k nur permutiert. Da also jede Permutation der V einer Permutation der x entspricht, so sind die elementarsymmetrischen Funktionen dieser V symmetrische Funktionen von $x_1, \ldots, x_n$ und daher Polynome in $c_1, \ldots, c_n$ mit ganzen Koeffizienten. Sind demnach $c_1, \ldots, c_n$ in K enthalten, so sind auch die Koeffizienten des Polynoms

$$(4) \qquad P(V)=(V-V_1)(V-V_{s_2})\ldots(V-V_{s_r})$$

Größen aus K.

Wenn $P(V)$ in K reduzibel ist, so möge $G(V)$ derjenige in K irreduzible Faktor sein, für den $G(V_1)=0$. Ist $P(V)$ in K irreduzibel, so sei $G(V)=P(V)$. In beiden Fällen ist $G(V)=0$ eine in K irreduzible Gleichung mit der Wurzel V_1; sie heißt eine Galoissche Resolvente der Gleichung (1) für den Körper K.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

So sind

$$G(V) \equiv (V - V_1)(V - V_c) \equiv V^2 - 2V + 2$$

bzw.

$$G(V) \equiv V - V_1$$

Resolventen der Gleichung von 88., Beispiel 1 für den Körper R (d. h. den Körper der rationalen Zahlen) bzw. den Körper $R(i)$.

Satz 2: $x_1, \ldots, x_n$ seien die Wurzeln einer Gleichung aus K und $\varphi(x_1, \ldots, x_n)$ sei ein Polynom aus K. Ferner sei s eine Substitution der Wurzeln, welche φ durch φ_s und die $n!$ wertige Funktion V_1 durch V_s ersetzt. Dann läßt sich φ_s darstellen als

$$\varphi_s = \frac{\lambda(V_s)}{P'(V_s)}, \tag{5}$$

wo λ ein Polynom aus K und P' die Ableitung des Polynoms (4) aus K ist, so daß $P'(V_s) \neq 0$. Es ist also φ_s dieselbe rationale Funktion $\varrho(V_s)$ von V_s wie $\varphi \equiv \varphi_1$ von V_1.

Es sei $r = n!$, $l = s_r$. Offenbar werden $\varphi_1, \ldots, \varphi_l$ durch s_k ebenso permutiert wie $V_1, \ldots, V_l$, so daß die Funktion

$$\lambda(V) \equiv \varphi_1 \frac{P(V)}{V - V_1} + \cdots + \varphi_l \frac{P(V)}{V - V_l} \tag{6}$$

durch s_k ungeändert bleibt. Ersetzt man $P(V)$ durch seinen Wert aus (4), so sieht man, daß $\lambda(V)$ ein Polynom in V wird, dessen Koeffizienten ganze rationale symmetrische Funktionen von $x_1, \ldots, x_n$ aus K, also selbst Größen aus K sind. Für $V = V_s$ verschwindet jeder Bruch mit Ausnahme desjenigen mit dem Nenner $V - V_s$. Der Quotient von (4) und $V - V_s$ ist für $V = V_s$ aber nichts anderes als der Wert der Ableitung von (4) für $V = V_s$, so daß

$$\lambda(V_s) = \varphi_s \cdot P'(V_s).$$

Sollte der Grad der Galoisschen Resolvente $G(V) = 0$ kleiner als $n!$ sein, so können wir zwar Zähler und Nenner von $\varphi_1 = \frac{\lambda(V_1)}{P'(V_1)}$ vermittels $G(V_1) = 0$ als Polynome niedrigeren Grades in V_1 ausdrücken, so daß dann $\varphi_1 = r(V_1)$ wird. Jetzt folgt aber nicht wie oben, daß wir aus $\varphi_1 = r(V_1)$ durch Anwendung irgendeiner Substitution s wieder eine richtige Beziehung $\varphi_s = r(V_s)$ bekommen; denn um eine solche zu erhalten, müßten wir den Bruch (5) mittels $G(V_s) = 0$ reduzieren; ob aber $G(V_s)$ wirklich gleich Null ist, wissen wir nicht, es müßte denn s eine jener Substitutionen sein, für die V_s eine Wurzel von $G(V) = 0$ ist; für jede andere Substitution s ist V_s eine Wurzel eines anderen Faktors von $P(V)$ in (4). — Diese Bemerkung führt zu einem kritischen Punkt unserer ganzen Theorie und zeigt, wie sorgfältig wir bei unseren Untersuchungen vorgehen müssen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

90. Die Gruppe einer Gleichung für einen gegebenen Körper. Die Koeffizienten einer Gleichung (1) mit lauter verschiedenen Wurzeln $x_1, \ldots, x_n$ mögen in K liegen. Ferner seien

$$V_1, V_a, V_b, \ldots, V_p \tag{7}$$

die Wurzeln einer Galoisschen Resolvente $G(V) = 0$ vom Grade g; die Indizes deuten dabei diejenigen Substitutionen von $x_1, \ldots, x_n$ an, vermöge deren diese V aus V_1 hervorgehen.

Satz 3: Diese g Substitutionen

$$G: 1, a, b, \ldots, p \tag{8}$$

bilden eine Gruppe, die sog. Galoissche Gruppe der gegebenen Gleichung (1) für den Bereich K.

Der Beweis kommt darauf hinaus, zu zeigen, daß mit r und s auch rs in (8) vorkommt oder daß mit V_r und V_s auch V_{rs} eine der Wurzeln (7) von $G(V) = 0$ ist. — Es ist also $G(V_r) = 0$, oder — wenn wir Satz 2 für $\varphi = V_r$ anwenden, da dann $V_r = \frac{\lambda(V_1)}{P'(V_1)}$ — es hat die Gleichung

$$G\left(\frac{\lambda(V)}{P'(V)}\right) = 0$$

die Wurzel $V = V_1$. Multipliziert man die linke Seite mit der $g$ten Potenz von $P'(V)$, so erhält man ein Polynom $H(V)$ aus K, welches für $V = V_1$ verschwindet. Nach 82. ist daher auch die Wurzel V_s der in K irreduziblen Gleichung $G(V) = 0$ eine Wurzel von $H(V) = 0$, oder, wenn wir $H(V_s)$ durch die $g$te Potenz von $P'(V_s) \neq 0$ dividieren, es ist

$$0 = G\left(\frac{\lambda(V_s)}{P'(V_s)}\right) = G(V_{rs}),$$

da

$$V_{rs} = (V_r)_s = \left(\frac{\lambda(V_1)}{P'(V_1)}\right)_s.$$

V_{rs} ist also wie behauptet eine Wurzel von $G(V) = 0$.

Beispiel: In 89. sahen wir, daß V_1 und V_c die Wurzeln einer Galoisschen Resolvente von $x^3 + x^2 + x + 1 = 0$ für den Körper R sind, d. h. die Gruppe dieser Gleichung besteht für R aus $\{1, (x_2 x_3)\}$. Für den Körper $R(i)$ hingegen ist $V - V_1 = 0$ eine Galoissche Resolvente, und die Gruppe besteht nur aus der identischen Substitution.

91. Charakteristische Eigenschaften der Galoisschen Gruppe einer Gleichung.

A. Wenn eine rationale Funktion der Wurzeln einer Gleichung aus K bei allen Substitutionen der Gleichungsgruppe ihren Wert beibehält, so ist sie eine Größe aus K.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die Funktion sei $\frac{\varphi}{\psi}$, wo φ und ψ Polynome in den Wurzeln mit Koeffizienten aus K sind. Die Koeffizienten von ψ sind natürlich auf Werte beschränkt, für die $\psi \equiv \psi_1 \neq 0$. Nun ist nach Satz 2

$$\psi_s = \frac{\mu(V_s)}{P'(V_s)}$$

und, da $\psi_1 \neq 0$, so ist auch $\mu(V_1) \neq 0$. Desgleichen ist $\psi_s \neq 0$, denn wenn $\mu(V) = 0$ die Wurzel V_s hätte, so hätte es auch die Wurzel V_1 mit $G(V) = 0$ gemeinsam (82.). Daher sind alle Funktionen

$$\frac{\varphi_s}{\psi_s} = \frac{\lambda(V_s)}{\mu(V_s)} \quad \text{für} \quad s = 1, \alpha, \ldots, \rho$$

definiert. Sind diese Funktionen alle gleich, ist mit anderen Worten $\frac{\varphi}{\psi}$ gegenüber den Substitutionen von G invariant, so ist

$$\frac{\varphi}{\psi} = \frac{1}{g}\left[\frac{\lambda(V_1)}{\mu(V_1)} + \frac{\lambda(V_\alpha)}{\mu(V_\alpha)} + \cdots + \frac{\lambda(V_\rho)}{\mu(V_\rho)}\right].$$

Die rechte Seite ist eine rationale symmetrische Funktion mit Koeffizienten aus K der Wurzeln von $G(V) = 0$ und daher eine rationale Funktion der zu K gehörenden Koeffizienten von $G(V)$, d. h. $\frac{\varphi}{\psi}$ ist eine Größe aus K.

B. Wenn umgekehrt eine rationale Funktion der Wurzeln mit Koeffizienten aus K gleich einer Größe aus K ist, so bleibt sie bei allen Substitutionen von G ungeändert.

Es sei $\frac{\varphi}{\psi} = r$ eine Größe aus K. Dann verschwindet $\frac{\lambda(V)}{\mu(V)} - r$ für $V = V_1$, so daß die Gleichung $\lambda(V) - r \cdot \mu(V) = 0$ aus K auch von jeder anderen Wurzel V_s der irreduziblen Gleichung $G(V) = 0$ erfüllt wird (82.). Daher haben wir

$$r = \frac{\lambda(V_s)}{\mu(V_s)} = \frac{\varphi_s}{\psi_s} \quad \text{für} \quad s = 1, \ldots, \rho,$$

d. h. $\frac{\varphi}{\psi}$ wird durch die Substitutionen von G nicht geändert.

Da es unzählig viele $n!$ wertige Funktionen V_1 mit Koeffizienten aus einem gegebenen Körper K gibt, so gibt es auch unzählige Galoissche Resolventen $G(V) = 0$. Unsere Definition der Gruppe G der Gleichung ging aber von einer einzigen solchen Resolventen aus, die durch eine spezielle Wahl von V_1 bestimmt war. Indessen führen alle Funktionen V_1 zu derselben Gruppe, d. h. G ist ein-

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

deutig durch die gegebene Gleichung und den gegebenen Körper K bestimmt.

Dies folgt aus

Satz 4: Die Gruppe einer gegebenen Gleichung für einen gegebenen Körper K ist eindeutig durch die Eigenschaften A und B bestimmt.

Es sei zunächst $H = \{1, r, \ldots, m\}$ eine Gruppe mit der Eigenschaft A, d. h. jede rationale Wurzelfunktion, die sich gegenüber H invariant verhält, soll eine Größe aus K sein. Nun bleiben die Koeffizienten von

$$\varphi(V) \equiv (V - V_1)(V - V_r) \ldots (V - V_m)$$

als symmertische Funktionen von $V_1, V_r, \ldots, V_m$ durch die Substitutionen von H ungeändert und sind daher nach Voraussetzung Größen aus K. Da dann die Gleichung $\varphi(V) = 0$ Koeffizienten aus K besitzt und eine Wurzel V_1 der irreduziblen Galoisschen Resolvente $G(V) = 0$ enthält, so enthält sie alle deren Wurzeln, so daß $1, a, \ldots, p$ unter den Substitutionen von H vorkommen und daher G eine Untergruppe von H ist.

Ferner sei $I = \{1, s, \ldots, t\}$ eine Gruppe mit der Eigenschaft B, d. h. sie soll alle Größen aus K ungeändert lassen. Dann bleibt die Funktion $G(V_1)$, da sie gleich der Zahl Null aus K ist, durch die Substitutionen von I ungeändert, so daß

$$0 = G(V_1) = G(V_s) = \cdots = G(V_t).$$

Es kommen also $V_s, \ldots, V_t$ unter den Wurzeln von $G(V) = 0$ vor, und daher ist I eine Untergruppe von G.

Sollen beide Eigenschaften A und B für eine Gruppe zutreffen, so kann sie daher nur gleich G selbst sein.

Mit Rücksicht auf die zahlreichen Anwendungen halten wir das zweite obige Resultat in dem Satz fest:

Satz 5: Wenn jede rationale Funktion der Wurzeln mit Koeffizienten aus K, welche gleich einer Größe aus K ist, durch jede Substitution einer Gruppe I ungeändert bleibt, so ist I eine Untergruppe der Gruppe der Gleichung.

92. Transitive und reguläre Gruppen. Eine Substitutionsgruppe von $x_1, \ldots, x_n$ heißt transitiv, wenn in ihr Substitutionen s_i vorkommen, die x_1 durch x_i ersetzen für jedes i von 1 bis n. Sie enthält dann auch eine Substitution $s_i^{-1}s_j$, welche x_i durch x_j ersetzt. Eine Gruppe, die nicht transitiv ist, heißt intransitiv.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Eine transitive Gruppe $n$ter Ordnung von n Buchstaben heißt **regulär**; durch sie geht jedes Element einmal in jedes andere über.

Die symmetrische Gruppe von n Buchstaben und die Gruppe

$$G_4 = \{E, (12)(34), (13)(24), (14)(23)\} \tag{9}$$

von 4 Buchstaben sind z. B. beide transitiv. Letztere ist auch regulär, während es erstere für $n > 2$ nicht ist. — $\{E, (12), (34), (12)(34)\}$ ist eine intransitive Gruppe.

Satz 6: Die Ordnung einer transitiven Gruppe von n Buchstaben ist durch n teilbar.

Zunächst bilden alle Substitutionen, die x_1 ungeändert lassen, eine Untergruppe H. Wegen der Transitivität enthält G auch eine Substitution s_i, welche x_1 durch x_i ersetzt. Dann wird x_1 aber auch durch jede Substitution des Komplexes Hs_i in x_i übergeführt. In

$$\Gamma = H + Hs_2 + Hs_3 + \cdots + Hs_n$$

ist daher jede Substitution des Komplexes Hs_i von jeder Substitution des Komplexes Hs_j verschieden. Andererseits kommt aber jede Substitution t von G in einem der Komplexe Hs_i vor; denn wenn x_1 durch t in x_k übergeht, so bleibt x_1 durch ts_k^{-1} ungeändert und ist daher eine Substitution h aus H, d. h. es ist $t = hs_k$. — Also ist $G = \Gamma$, und die Ordnung von G ist gleich dem Produkt der Ordnung von H und n.

Satz 7: Wenn eine Gleichung in K irreduzibel ist, so ist ihre Gruppe für K transitiv, und umgekehrt.

Es sei $f(x) = 0$ in K irreduzibel. Angenommen, seine Gruppe G für K sei intransitiv und enthalte daher zwar Substitutionen, welche x_1 durch $x_1, x_2, \ldots, x_m$, aber keine, welche x_1 durch eine der Größen $x_{m+1}, \ldots, x_n$ ersetzen. Greifen wir irgendeine Substitution s aus G heraus, welche $x_i (i \leqq m)$ in x_j überführt. Da G eine Substitution t enthält, welche x_1 durch x_i ersetzt, so enthält sie auch ts, welches x_1 in x_j überführt. Daher ist $j \leqq m$, und s permutiert $x_1, \ldots, x_m$ nur untereinander, läßt also jede symmetrische Funktion von ihnen ungeändert. Dann folgt aus 91. A., daß die Koeffizienten von

$$g(x) \equiv (x - x_1)(x - x_2) \ldots, (x - x_m)$$

Größen aus K sind. Es wäre also $g(x)$ in $f(x)$ enthalten, was der Irreduzibilität von $f(x)$ widerspricht.

Um die Umkehrung zu beweisen, setzte man G als transitiv und $f(x)$ als reduzibel in K voraus. Dann besitzt $f(x)$ einen Faktor $g(x)$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

aus K vom Grade $m < n$, so daß $g(x_1) = 0$ ist. Eigenschaft B zeigt dann, daß $g(x_1)$ bei jeder Substitution von G seinen Wert, nämlich Null, beibehält. Da G transitiv ist, so enthält es eine Substitution, die x_1 in $x_i (i \leqq n)$ überführt, es wäre also $g(x_i) = 0$ für jedes i von 1 bis n.

Beispiel: Man finde die Gruppe von $x^3 - 7x + 7 = 0$ für R. — Da nach 83., Beispiel 3 die Gleichung in R irreduzibel ist, so ist G transitiv. Nach 69. ist das Quadrat von

$$\psi = (x_2 - x_3)(x_3 - x_1)(x_1 - x_2) \tag{10}$$

gleich der Diskriminante 49 unserer Gleichung, so daß ψ entweder $+7$ oder -7, auf jeden Fall also eine Zahl aus R ist. Da jede Transposition ψ in $-\psi$ überführt, so ist sie wegen B nicht in G enthalten. Diese beiden Ergebnisse zeigen, daß $G = \{E, (123), (132)\}$.

Übungen: 1. Wenn eine Gleichung eine rationale Wurzel x_1 (aber wie immer keine mehrfache Wurzel) besitzt, so bleibt x_1 bei beliebigem Bereich K durch jede Substitution der Galoisschen Gruppe ungeändert (nach Eigenschaft B). Wenn eine Wurzel x_j nicht zu K gehört, so enthält die Gruppe eine Substitution, welche x_j ändert. Hiermit beweise man, daß in R die Gruppe von $(x - 1)(x + 1)(x - 2) = 0$ die Identität ist; ebenso daß in R die Gruppe von $x^3 - 1 = 0$ die Ordnung 2 besitzt.

2. Die Gruppe von $x^3 - 9x + 9 = 0$ in R hat die Ordnung 3. Denn der Wert von (10) ist hier ± 27.

3. Die Gruppe von $x^3 - 2 = 0$ für den Bereich $R(\omega)$, wo ω eine imaginäre kubische Einheitswurzel ist, ist von der Ordnung 3.

Vgl. wieder (10), welches hier gleich $\pm 6\sqrt{-3}$ wird, also in $R(\omega)$ liegt.

4. Die Gruppe von $x^3 - 2 = 0$ für R ist die symmetrische Gruppe. Denn wenn sie die alternierende Gruppe wäre, so hätte (10) einen rationalen Wert.

5. Man suche die Gruppe G von $x^4 + 1 = 0$ für R. Nach 73., Beispiel 1 sind $y_1 = x_1x_2 + x_3x_4$, y_2 und y_3 die (rationalen) Wurzeln $0, \pm 2$ der Resolvente $y^3 - 4y = 0$. Eigenschaft B zeigt, daß y_1, y_2, y_3 durch jede Substitution s von G ungeändert bleibt. Nach 75., Beispiel 4 gehört daher s zu der Gruppe (9). Da schließlich (82., Beispiel 4) $x^4 + 1$ in R irreduzibel ist, so ist G transitiv und daher von der Ordnung $\geqq 4$, d. h. es ist $G = G_4$.

6. Die Gruppe von $x^4 + 1 = 0$ in $R(i)$ ist von zweiter Ordnung. — Denn die Faktoren $x^2 \pm i = 0$ zeigen, daß die Gruppe eine intransitive Untergruppe von (9) ist.

7. Wenn $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$ rationale Koeffizienten hat und in R irreduzibel ist, so gelten die Sätze:

a) Wenn die Gleichung eine komplexe Wurzel x_1 vom absoluten Betrage 1 hat, so ist sie reziprok und von grader Ordnung. — Denn zunächst ist $\bar{x}_1$ auch eine Wurzel, etwa x_2, und es ist $x_1x_2 = 1$. Die Gruppe der Gleichung

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ist transitiv, und zwar verändert jede Substitution aus G sowohl x_1 als x_2, weil sonst die Gleichung eine mehrfache Wurzel hätte, also reduzibel wäre; ich bekomme so die neue Gleichung $x_3 x_4 = 1$. Usw.

b) Wenn es eine Wurzel $r + is$ mit rationalem reellem Bestandteil r gibt, so ist n grade und die n Wurzeln können so zu Paaren zusammengestellt werden, daß bei jedem Paar die Summe konstant $2r$ ist, wo $r = -a_1 : n a_0$. Insbesondere enthält also die Gleichung für $r = 0$ nur grade Potenzen von x. — Der Beweis verläuft ähnlich wie oben.

c) Wenn es eine imaginäre Wurzel $a + bi$ gibt, für die $a^2 + b^2$ rational ist, so ist n grade, und die n Wurzeln können so zu Paaren zusammengestellt werden, daß das Produkt je zweier zusammengehöriger Wurzeln gleich $a^2 + b^2$ ist. Ist ϱ eine Quadratwurzel von $a^2 + b^2$, so ist $\varrho^n = a_n : a_0$. Schließlich wird die Gleichung in y reziprok, wenn man in ihr x durch ϱy ersetzt.

8. Für R ist die Gruppe von $x^4 + x^3 + x^2 + x + 1 = 0$ zyklisch und von der Ordnung 4. Nach 85., Beispiel 2 ist die Gleichung in R irreduzibel. — Die Erzeugende der Gruppe ist (1234).

9. G sei für K die Gruppe einer in K irreduziblen Gleichung, deren Wurzeln r_i rationale Funktionen $f_i(r_n)$ einer von ihnen mit Koeffizienten aus K sind. ($i = 0, 1, \ldots, n-1$.) Man beweise, daß G regulär und daß $f_i[f_j(r_n)]$ ebenfalls eine Wurzel ist. — Jede Substitution aus G führt die Gleichung $r_i - f_i(r_n) = 0$ wieder in eine richtige Gleichung $r_k - f_i(r_l) = 0$ über. Dabei ist $l \neq n$, da sonst die Gleichung mehrfache Wurzeln hätte. Ebenso $i \neq k$. Keine Substitution der transitiven Gruppe G läßt also irgendeine Wurzel unverändert, d. h. G ist regulär. Es gibt daher eine Substitution, die in $r_i - f_i(r_n) = 0$ r_n durch r_j ersetzt:

$$r_k - f_i(r_j) = 0 \quad \text{oder} \quad r_k - f_i[f_j(r_n)] = 0.$$

93. Rationale Funktionen, die zu einer Gruppe gehören. Man betrachte eine in K rationale Funktion $\psi(x_1, \ldots, x_n)$ der Wurzeln einer Gleichung aus K. Es seien $1, a, b, \ldots, k$ alle die Substitutionen ihrer Galoisschen Gruppe G, welche ψ seinem Werte nach ungeändert lassen. Wegen $\psi - \psi_a = 0$ ist nach B auch $\psi_b - \psi_{ab} = 0$, d. h. $\psi = \psi_{ab}$. Der Komplex $1, a, b, \ldots, k$ enthält also auch ab, ist demnach eine Gruppe H. Man sagt: ψ gehört zu der Untergruppe H von G.

Beipiel: x_1 und $x_2 = -x_1$ seien zwei Wurzeln von $x^4 + 1 = 0$. Die einzigen Substitutionen ihrer Gruppe (9) für R, welche x_1^2 ungeändert lassen, sind E und (12)(34). Sie bilden daher die Untergruppe, zu der x_1^2 gehört.

Umgekehrt gibt es aber auch zu jeder Untergruppe H gewisse Funktionen, die zu ihr gehören. Denn ist V_1 irgendeine $n!$wertige Funktion der Wurzeln mit Koeffizienten aus K und sind $V_1, V_a, \ldots, V_k$ die Funktionen, die aus V_1 durch die Substitutionen

Digitized by Google Original from UNIVERSITY OF MICHIGAN

von H hervorgehen, so können wir eine ganze Zahl r finden, so daß

$$\psi \equiv (r - V_1)(r - V_a) \ldots (r - V_k)$$

zu H gehört. Denn wenn s irgendeine Substitution von H ist, so ist $s, as, \ldots, ks$ nur eine andere Anordnung der Substitutionen von H. Daher ist ψ gleich

$$\psi_s \equiv (r - V_s)(r - V_{as}) \ldots (r - V_{ks}).$$

Wenn aber t eine nicht in H liegende Substitution von G ist, so ist ψ_t nicht für alle Werte von r mit ψ identisch, da V_t von V_1, $V_a, \ldots, V_k$ verschieden ist und wir wie in 88. eine ganze Zahl r so wählen können, daß jedes ψ_t von ψ verschieden ist. D. h. ψ gehört zu H. — Wir haben also

Satz 8: Jede rationale Funktion ψ mit Koeffizienten aus K der Wurzeln einer Gleichung, die für K die Gruppe G besitzt, gehört zu einer bestimmten Untergruppe von G. Umgekehrt gibt es zu jeder Untergruppe von G solche Funktionen ψ.

Wir beweisen sogleich den wichtigen Ergänzungssatz:

Satz 9: Wenn eine in K rationale Funktion ψ der Wurzeln einer Gleichung, welche für K die Gruppe G besitzt, zu einer Untergruppe H vom Index u unter G gehört, so wird ψ durch die Substitutionen von G in genau u verschiedene Funktionen übergeführt, die sogenannten ***Konjugierten*** *von ψ unter G. Sie sind die Wurzeln einer in K irreduziblen Gleichung mit Koeffizienten aus K.*

Man zerlege G in

$$G = H + Hg_2 + Hg_3 + \cdots + Hg_u \tag{11}$$

(vgl. 78.). Ist dann h irgendeine Substitution von H, so ist

$$\psi_{hg_i} = (\psi_h)_{g_i} = \psi_{g_i} \equiv \varphi_i,$$

so daß ψ höchstens u Werte annehmen kann. Andererseits sind diese Werte alle voneinander verschieden, denn wenn $\psi_i = \psi_k$ wäre, so wäre auch $\psi_p = \psi$, wo also $p = g_i g_k^{-1}$ zu H gehörte, da es ψ ungeändert läßt. Dann wäre aber auch $Hg_i = Hpg_k = Hg_k$, was nur für $i = k$ möglich ist.

Nun werden $\psi_1, \ldots, \psi_u$ durch jede Substitution s von G lediglich permutiert. Denn weil $g_i s$ nach (11) in die Form hg_k gebracht werden kann, so ist

$$(\psi_i)_s = \psi_{g_i s} = \psi_{hg_k} = \psi_{g_k} \equiv \psi_k.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Die elementarsymmetrischen Funktionen der ψ, die abgesehen vom Vorzeichen gleich den Koeffizienten des Polynoms

$$g(y) \equiv (y - \psi_1)(y - \psi_2) \ \ldots \ (y - \psi_u) \tag{12}$$

sind, verhalten sich demnach s gegenüber invariant. Nach 91. A. sind sie daher Größen aus K.

Wenn nun $g(y)$ in K reduzibel wäre, so wäre für denjenigen Faktor $t(y)$, der für $y = \psi_1$ verschwindet, nach 91. B. auch $t(\psi_2) = 0, \ldots, t(\psi_u) = 0$; d. h. es ist $t(y) \equiv g(y)$, $g(y)$ also irreduzibel.

Beispiel 1: Die Gruppe von $x^3 + x^2 + x + 1 = 0$ für R ist, wenn die Wurzel -1 mit x_1 bezeichnet wird, $\{E, (23)\}$. Die Konjugierten von $\psi = x_2 - x_1$ unter G sind $\psi_1 = \psi$ und $\psi_2 = x_3 - x_1$. Sie sind die Wurzeln der in R irreduziblen Gleichung $y^2 - 2y + 2 = 0$.

Beispiel 2: Die Gruppe von $x^4 + 1 = 0$ für $R(i)$ ist $\{E, s\}$, wo s ein Produkt von 2 Transpositionen ist (vgl. 92., Beispiel 6). Man setze $x_1 = \varrho$, $x_2 = i\varrho$, $x_3 = -\varrho$, $x_4 = -i\varrho$, wo $\varrho = \frac{1}{2}(i+1)\sqrt{2}$ und daher $\varrho^2 = i$ ist; ferner sei $s = (13)(24)$. Die konjugierten x_1 und x_3 unter G sind die Wurzeln von $y^2 - i = 0$, welche Gleichung in $R(i)$ irreduzibel ist, da ϱ nicht in diesem Bereich vorkommt.

Satz 10[1]: Wenn ψ eine zu der Untergruppe H gehörige Funktion der Wurzeln einer Gleichung mit Koeffizienten aus K ist, so läßt sich jede andere Funktion φ aus K, die bei den Substitutionen von H ungeändert bleibt, als rationale Funktion von ψ mit Koeffizienten aus K darstellen.

$\psi_1, \ldots, \psi_u$ seien die Konjugierten von $\psi = \psi_1$ unter G. Da jede Substitution h von H die Funktion φ ungeändert läßt, so wird φ durch jedes Produkt hg_i in $\varphi_i \equiv \varphi_{\vartheta_i}$ übergeführt. Nach dem Beweis von Satz 9 wird ψ_i durch jede Substitution s von G in eine gewisse Funktion ψ_k übergeführt, und ähnlich φ_i in φ_k. Ist daher $g(y)$ durch (12) definiert, so werden in

$$\lambda(y) \equiv g(y)\left(\frac{\varphi_1}{y - \psi_1} + \frac{\varphi_2}{y - \psi_2} + \cdots + \frac{\varphi_u}{y - \psi_u}\right)$$

die Brüche durch s lediglich permutiert. Die Koeffizienten auf der rechten Seite bleiben also bei allen Substitutionen von G ungeändert, d. h. $\lambda(y)$ liegt in K. Setzt man $\psi_1 \equiv \psi$ für y ein, so erhält man (ähnlich wie bei Satz 2)

$$\varphi = \lambda(\psi) : g'(\psi).$$

1) Für den Fall, daß die Wurzeln unabhängige Variablen sind, ist der Satz von Lagrange bewiesen worden. Nouv. Mém. Acad. Berlin, années 1770—71; §§ 100—104; Œuvres III, pp. 374—388.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Beispiel: ψ sei eine $n!$ wertige Funktion V_1, so daß die identische Substitution E die einzige ist, der gegenüber ψ sich invariant verhält. Da E jedes φ ungeändert läßt, so zeigt Satz 10, daß jede rationale Funktion φ mit Koeffizienten aus K sich als rationale Funktion von V_1 mit Koeffizienten aus K darstellen läßt. (Vgl. auch 89.)

94. Erniedrigung der Gruppe durch Erweiterung des Körpers. G sei die Gruppe von $f(x) = 0$ für einen Körper K, der die Koeffizienten von $f(x)$ enthält. Der Körper $K' = K(\psi)$, der aus den rationalen Funktionen von ψ mit Koeffizienten aus K besteht, heißt aus K durch Adjunktion von ψ zu K entstanden (79.). Wenn die irreduzible Galoissche Resolvente $G(V) = 0$ für K auch in K' irreduzibel bleibt, so ist G offenbar auch die Gruppe für K'; sollte sie aber in K' reduzibel werden, so sei $G'(V)$ derjenige in K' irreduzible Faktor von $G(V)$ mit Koeffizienten aus K', der für $V = V_1$ verschwindet. Sind dann $V_1, V_a, \ldots, V_k$ die Wurzeln von $G'(V) = 0$, so ist für K' die Gruppe von $f(x) = 0$ definitionsgemäß $G' = \{E, a, \ldots, k\}$, also eine Untergruppe von G. — Wir haben so

Satz 11: Durch eine Adjunktion zu dem Stammkörper erniedrigt sich die Gruppe einer Gleichung auf eine ihrer Untergruppen.

Beispiel 1: Für R besteht die Gruppe von $x^3 + x^2 + x + 1 = 0$ aus $\{E, (23)\}$, wenn x_1 die Wurzel -1 bezeichnet. Im erweiterten Bereich $R(i)$ jedoch besteht die Gruppe nur aus E. (Beisp. in 90.). — Man beachte, daß die adjungierte Größe $i = x_2$ zu der Untergruppe E von G gehört.

Beispiel 2: $x^4 + 1 = 0$ besitzt in R die Gruppe G_4 von (9). Mit den Bezeichnungen von 93., Beispiel 2 ist für $R(i)$ die Gruppe gleich $G_2 = \{E, (13)(24)\}$. Letztere ist die Untergruppe von G_4, zu der $i = x_1^2 = x_3^2 = -x_2^2 = -x_4^2$ gehört.

Diese Beispiele erläutern den wichtigen Satz:

Satz 12: Wenn ψ eine in K rationale Funktion der Wurzeln ist und zu der Untergruppe H von G gehört, so reduziert sich durch Adjunktion von ψ zu K die Galoissche Gruppe von G auf H.

Wir haben zu beweisen, daß H in $K' = K(\psi)$ die charakteristischen Eigenschaften A und B der Gruppe der Gleichung hat. Offenbar ist jede rationale Funktion φ der Wurzeln mit Koeffizienten aus K' auch gleich einer rationalen Funktion φ_1 der Wurzeln mit Koeffizienten aus K.

φ sei eine Funktion, die bei allen Substitutionen von H ungeändert bleibt. Nach Satz 10 ist dann $\varphi_1 \equiv \varphi$ eine rationale Funktion von ψ mit Koeffizienten aus K. Daher liegt φ_1 in $K' = K(\psi)$, so daß f für H und K' die Eigenschaft A besteht.

Jetzt sei φ gleich einer Größe r in K', nämlich eine rationale Funktion $r(\psi)$ mit Koeffizienten aus K. Dann ist $\varphi_1 - r(\psi)$ eine

Digitized by Google Original from UNIVERSITY OF MICHIGAN

rationale Funktion der Wurzeln mit Koeffizienten aus K, welche den Wert Null hat und daher bei jeder Substitution von G, also auch von H, ungeändert bleibt, und da $r(\psi)$ sich gegenüber H invariant verhält, so ist auch $\varphi_1 = \varphi$. Es besteht also für H und K' auch die Eigenschaft B.

Übungen: 1. Durch Adjunktion von $\sqrt{2}$ zu $R(i)$ reduziert sich die Gruppe G_2 von $x^4 + 1 = 0$ auf E.

2. Durch Adjunktion einer imaginären kubischen Einheitswurzel ω zu R reduziert sich die Gruppe G_6 von $x^3 - 2 = 0$ auf die zyklische Gruppe C_3 (92., Beispiel 3, 4). Man bestätige, daß $\omega = x_2 : x_1$ zu C_3 gehört. Durch die weitere Adjunktion von $\sqrt[3]{2}$ reduziert sich die Gruppe auf E.

3. Man suche die Gruppe von $x^4 + x^3 + x^2 + x + 1 = 0$ für den Körper $R(\sqrt{5})$.

95. **Die Gruppe der allgemeinen Gleichung.** Die Koeffizienten $c_1, \ldots, c_n$ von (1) seien unabhängige komplexe Variabeln. $x_1, \ldots, x_n$ seien die Wurzeln im Sinne von 81. Dann gilt

Satz 13: Für den Körper K, der durch die Koeffizienten der allgemeinen Gleichung und durch irgendwelche, aber endlich viele Konstanten bestimmt ist, ist die Gruppe der Gleichung die symmetrische Gruppe.

Angenommen, die Gruppe sei $H = \{1, a, \ldots, k\}$ und enthalte nicht die Substitution s. Abgesehen vom Vorzeichen sind die elementarsymmetrischen Funktionen von $V_1, V_a, \ldots, V_k$ die Koeffizienten der Galoisschen Resolvente und sind daher Größen in K. Liegt also r in K, so liegt auch

$$\psi \equiv (r - V_1)(r - V_a) \ldots (r - V_k)$$

in K. Wie in 93., so können wir auch hier einen ganzzahligen Wert von r so wählen, daß $\psi_s \neq \psi$. Andererseits ist ψ, da es in K liegt, rational durch $c_1, \ldots, c_n$ ausdrückbar und wird daher durch s nicht geändert. Durch die Annahme, s komme nicht in H vor, sind wir also auf einen Widerspruch gestoßen.

96. **Weitere Ergebnisse.** Hilbert[1]) bewies durch eine eingehende Untersuchung, daß, wenn f ein in R irreduzibles Polynom in $x_1, \ldots, x_n, t_1, \ldots, t_s$ mit ganzen Koeffizienten ist, man immer auf unzählig viele Weisen ganzzahlige Werte für die t_j finden kann, so daß f eine Funktion der x_i wird, die auch jetzt noch in R irreduzibel ist. Ist $\varphi(x) = 0$ eine Gleichung in x, deren Koeffizienten ganzzahlige Polynome in $t_1, \ldots, t_s$ sind, so können wir den t_j ganzzahlige Werte beilegen, so daß die resultierende Gleichung in x dieselbe Gruppe für R hat wie $\varphi(x) = 0$. — Auf die allgemeine

1) Journ. f. Math. 110, 1892, pp. 104—129.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Gleichung angewendet heißt dies: es gibt unzählig viele Gleichungen vom $n$ten Grade mit ganzen Koeffizienten, deren Gruppe für R die symmetrische ist. — Ähnliches gilt für die alternierende Gruppe. — Die beiden letzten Resultate wurden auf mannigfache Weise einfacher bewiesen.[1])

Neuerdings[2]) hat man auch das Problem in Angriff genommen, alle Gleichungen $n$ten Grades mit vorgeschriebener Gruppe zu finden, und ist in den Fällen $n = 3$, $n = 4$ zu bestimmten Ergebnissen gekommen.

Eine Gleichung, deren Koeffizienten rationale Funktionen einer komplexen Variabeln t sind, besitzt eine Gruppe mit einer invarianten Untergruppe, der Monodromiegruppe, die aus allen Substitutionen der Wurzeln besteht, die entstehen, wenn t in der komplexen Ebene[3]) eine geschlossene Kurve durchläuft. — Ähnlich existiert eine Monodromiegruppe einer linearen Differentialgleichung, wenn man an Stelle der Wurzeln jetzt linear unabhängige Integrale wählt.

Ebenso hat man die Gruppe eines Systems algebraischen Gleichungen studiert.[4]) Desgleichen die Gruppen einer reziproken Gleichung vierten Grades[5]) und der auflösbaren Moivreschen[6]) Gleichung fünften Grades.[7])

1) Weber, Math. Papers Chicago Congress 1896, pp. 401—407; Algebra, 2. Ausg., I 1898, pp. 653—655. Maillet, Journ. de Math. (5), 5, 1899, pp. 205 bis 216. Bauer, Journ. für Math. 132, 1907, pp. 33—35; Math. Annalen 64, 1907, pp. 325—327. Schur, Jahresbericht Deutsch. Math. Vereing. 29, 1920, pp. 145—150. Furtwängler, Math. Annalen 85, 1922, pp. 34—40.

2) E. Noether, Math. Annalen 78, 1918, pp. 221—229. Seidelmann, ibid., pp. 230—233. Breuer, ibid. 86, 1922, pp. 108—113 (zyklische Gleichungen sechsten Grades).

3) Miller, Blichfeldt u. Dickson, Finite Groups, pp. 378—381. Hermite, Comptes rend. Paris, 32, 1851 (Œuvres I, pp. 276—280). Frobenius, Journ. f. Math. 74, 1872, pp. 254—272. Kneser, Irreduzibilität und Monodromiegruppe algebraischer Gleichungen, Dissertat., Berlin 1885; Math. Annal. 28, 1886, pp. 125—132. Hurwitz, ibid. 39, 1891, p. 23. Bianchi, Teoria d. Gruppi di Sostitutioni, 1897, pp. 314—323. Baker, Annals of Math. 14, 1912—13, pp. 119—136. Ritt, Trans. Amer. Math. Soc. 24, 1922, pp. 21—30.

4) Weisner, Bull. Amer. Math. Soc. 30, 1924, pp. 314—316. (Die Problemstellung verdankt man König, Math. Annalen 18, 1881, pp. 69—77.)

5) Dickson u. Börger, Amer. Math. Monthly 15, 1908, p. 71—78, pp. 85 bis 87. Miller, Blichfeldt u. Dickson, Finite Groups, 1916, p. 291. Kriterien für die Irreduzibilität reziproker Gleichungen vom Grade $2n$ finden sich in: Dickson, Bull. Amer. Math. Soc., 14, 1907—08, pp. 426—430.

6) Phil. Trans. London 25, 1707, pp. 2368—70.

7) Börger, Amer. Math. Monthly 15, 1908, pp. 171—174.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Die Gruppe der Gleichung für die Wendepunkte einer ebenen Kurve dritter Ordnung ist von dem Verfasser[1]) ausführlich behandelt worden. Eine noch eingehendere Untersuchung[2]) ist für die 27 Geraden einer Fläche dritter Ordnung oder die 28 Doppeltangenten einer ebenen Kurve vierter Ordnung erforderlich.

Auch auf die gewöhnlichen linearen Differentialgleichungen[3]) sowie auf die vollständigen Systeme linearer partieller Differentialgleichungen ist die Galoissche Theorie ausgedehnt worden.[4])

---

1) Miller, Blichfeldt u. Dickson, Finite Groups, 1916, pp. 327—342; Annals of Math. 16, 1914, pp. 50—66.

2) Ibid., pp. 343—375. Auf den Seiten 375—377 befindet sich ein kurzer Bericht über Gruppen bei weiteren geometrischen Problemen.

3) Picard, Traité d'Analyse, III, Ch. 17. Loewy, H. Weber-Festschrift, 1912, pp. 198—227.

4) Vessiot, Annales Sc. École Normale Sup. (3), 21, 1904, pp. 1—85.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ELFTES KAPITEL.

AUFLÖSBARE GLEICHUNGEN.

97. Historisches. Euler, der führende Mathematiker des achtzehnten Jahrhunderts, glaubte noch, daß jede algebraische Gleichung durch Radikale (d. h. durch Wurzelziehen) lösbar sei. Von 1799 an gab jedoch Ruffini mehrere Versuche bekannt, mit Hilfe von Substitutionen der Wurzeln die Unlösbarkeit der allgemeinen Gleichung von höherem als viertem Grade zu beweisen. Sein endgültiger und einfachster Beweis[1]) ist im wesentlichen derselbe wie der, den man jetzt die „Wantzelsche Vereinfachung des Abelschen Beweises"[2]) nennt; nur eine triviale Bemerkung anstatt eines Beweises gab er indessen von dem jetzt nach Abel benannten Hilfssatze, daß, wenn eine Gleichung durch Radikale lösbar ist, die Wurzeln so dargestellt werden können, daß alle in ihren Ausdrücken vorkommenden Radikale rationale Funktionen der Wurzeln (und der Einheitswurzeln) mit rationalen Koeffizienten sind.

Der Abelsche Beweis[3]) dieses Satzes weist zwei Mängel auf: Wie W. R. Hamilton bemerkte[4]), ist die $n$te Wurzel von $q_\mu{}^n p^\mu$ im allgemeinen von höherer Ordnung als $p^{\frac{1}{n}}$. Dieser erste Mangel wird am besten dadurch beseitigt, daß man die unnötige Abelsche Klassifikation der Radikale ganz beiseite läßt. — Sodann enthält der Abelsche Beweis bei der Verwendung von Einheitswurzeln einen Fehler und wird verbessert, wenn man zu dem Rationalitätsbereich von Anfang an alle $k$ten Einheitswurzeln adjungiert, wobei k die Werte der Exponenten aller in dem Ausdruck für eine Wurzel y vorkommenden Radikale bezeichnet.

Um daher einen fehlerfreien Beweis für die Nichtauflösbarkeit von höherem als dem vierten Grade nach Art desjenigen von

1) Riflessioni intorno alla soluzione delle equationi algebraiche generali, Modena 1813.

2) Serret, Algèbre II, 4. oder 5. Ausg., p. 512.

3) Journ. f. Math. 1, 1826, pp. 65—84. Œuvres complètes I, 1881, pp. 66 bis 94.

4) Trans. Royal Irish Acad. 18, 1839, pp. 171—259. Eine sehr verwickelte Rekonstruktion des Abelschen Beweises.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Ruffini und Abel zu geben, müssen wir die Begriffe der Substitutionsgruppen und der Erweiterung eines Körpers durch Adjunktion heranziehen, welche Galois in seiner viel allgemeineren Theorie der Gleichungen anwandte.

98. Lösbarkeit durch Radikale. Die vier rationalen Operationen sind Addition, Subtraktion, Multiplikation und Division.

Eine algebraische Gleichung heißt durch Radikale lösbar (kurz: auflösbar), wenn alle ihre Wurzeln durch eine endliche Zahl von rationalen und von Wurzeloperationen gefunden werden können, wobei sich diese Operationen auf die Koeffizienten der Gleichung oder auf Größen erstrecken, die man aus ihnen durch die genannten Operationen erhält. Jede kubische und biquadratische Gleichung ist, wie wir in Kap. VIII sahen, durch Radikale lösbar. Eine unserer Hauptaufgaben ist die, zu entscheiden, ob auch jede Gleichung vom fünften oder höherem Grade durch Radikale lösbar ist.

Nach obiger Definition ist es uns gestattet, von einer vorher bestimmten Größe eine $p$te Wurzel, jedoch nicht alle solchen zu gebrauchen. Denn eine unserer Aufgaben besteht grade darin, zu beweisen, daß diese Einheitswurzeln, wenn p eine Primzahl ist, alle durch Radikale mit niedrigerem Index ausdrückbar sind.

Die Lösung einer durch Radikale lösbaren (kurz: auflösbaren) Gleichung wird gewöhnlich durch die Lösung einer Kette von Hilfsgleichungen herbeigeführt, wobei sich die Wurzeln jeder Gleichung aus ihren Koeffizienten und den Wurzeln der vorhergehenden Gleichungen rational und durch Wurzeloperationen ergeben. Um unsere Ausdrucksweise einer besonderen Gleichung der Kette zuwenden zu können und um eine anpassungsfähige Ausdrucksweise zu haben, ist es zweckmäßig, obige Definition folgendermaßen zu verallgemeinern:

Eine Gleichung mit Koeffizienten aus dem Körper $R(k_1, \ldots, k_m)$ soll in bezug auf diesen durch Radikale lösbar (kurz: auflösbar) heißen, wenn man alle ihre Wurzeln rational und durch Wurzelziehen aus $k_1, \ldots, k_m$ oder aus Größen, die aus ihnen durch diese Operationen entstehen, finden kann.

Bezeichnet z. B. ϱ eine imaginäre 13. Einheitswurzel, so ist $x^{13} = 2^{13}$ offenbar in bezug auf $R(\varrho)$ auflösbar.

99. Resolventengleichungen. Für den Bereich K sei G die Gruppe einer gegebenen Gleichung $f(x) = 0$ mit Koeffizienten aus K. Eine rationale Funktion ψ der Wurzeln mit Koeffizienten aus K gehört zu einer gewissen Untergruppe H vom Index u unter G.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Nach 93., Satz 5 ist ψ eine Wurzel einer Resolventengleichung vom Grade u mit Koeffizienten aus K. Angenommen, diese Gleichung sei bez. K auflösbar. Adjungiert man dann ihre Wurzeln zu K, so erhält man den Körper $K' = K(\psi)$, in bezug auf den jetzt die Gruppe von $f(x) = 0$ gleich H ist (94.). Führt eine Reihe solcher Adjunktionen zu einem Körper K_i, für den die Gruppe von $f(x) = 0$ gleich E ist, so gehören (wegen 91. A.) alle Wurzeln zu K_i.

Wir wollen zeigen, daß diese Voraussetzungen für $f(x) = x^3 + bx^2 + cx + d$ zutreffen, wenn b, c, d unabhängige Variabeln sind und $K = R(\omega, b, c, d)$ ist (ω = imaginäre kubische Einheitswurzel). Nach 95. ist G die symmetrische Gruppe G_6 der Wurzeln x_1, x_2, x_3. Zu der zyklischen Untergruppe C_3 gehört die alternierende Funktion

$$\delta = (x_2 - x_3)(x_3 - x_1)(x_1 - x_2),$$

deren Quadrat die Diskriminante Δ der kubischen Gleichung ist. Die Resolventengleichung $\delta^2 = \Delta$ ist bez. K auflösbar. Adjungiert man $\delta = \sqrt{\Delta}$ zu K, so erhält man den Körper $K_1 = K(\delta)$, für den die Gruppe unserer Gleichung C_3 ist. Führen wir dann die linearen Funktionen φ und ψ von 68. ein und erinnern uns dabei, daß wir in der darauf folgenden Übung zeigten, daß die Substitution (132) von C_3 die Funktion φ in $\omega\varphi$ und ψ in $\omega^2\psi$ überführte, so sehen wir, daß φ^3 und ψ^3 durch alle Substitutionen von C_3 ungeändert bleiben, daß sie also rationale Funktionen von δ mit Koeffizienten aus K sind (Satz 10 von 93.). Die Berechnungen in 68., 69. geben

$$\varphi^3 = \tfrac{1}{2}(B + 3\delta\sqrt{-3}) = g, \quad \psi^3 = \tfrac{1}{2}(B - 3\delta\sqrt{-3}) = h$$
$$\varphi\psi = b^2 - 3c,$$

wo $B = 9bc - 2b^3 - 27d$. Die Resolventengleichung $\varphi^3 = g$, wo g zu $K_1 = K(\delta)$ gehört, ist offenbar bez. K_1 auflösbar. Im erweiterten Körper $K_2 = K_1(\sqrt[3]{g})$ ist die Gruppe der gegebenen Gleichung die identische Gruppe, zu der φ gehört. Daher gehören alle Wurzeln x_i zu K_2; ihre Ausdrücke in Größen aus K_2 wurden in 68., (5) gegeben.

100. Die Gruppe einer Resolventengleichung. Für unsere spätere Erörterung über die Lösbarkeit der im Anfang von 99. definierten Resolventengleichung müssen wir deren Gruppe kennen. ψ gehöre zu der Untergruppe H vom Index u unter G. Mittels der Zerlegung

$$G = H + Hg_2 + Hg_3 + \cdots + Hg_u \tag{1}$$

bewiesen wir in 93., daß ψ eine der u verschiedenen unter G konjugierten Funktionen

$$\psi, \psi_{g_2}, \psi_{g_3}, \ldots, \psi_{g_u} \tag{2}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

ist und daß jede Substitution s von G diese lediglich permutiert, etwa zu

$$\psi_s, \psi_{g_2 s}, \psi_{g_3 s}, \ldots, \psi_{g_u s}. \tag{3}$$

Einer Substitution s von G der Buchstaben $x_1, \ldots, x_n$ entspricht daher die Substitution

$$\sigma = \begin{pmatrix} \psi & \psi_{g_2} & \cdots & \psi_{g_u} \\ \psi_s & \psi_{g_2 s} & \cdots & \psi_{g_u s} \end{pmatrix} \equiv \begin{pmatrix} \psi_{g_i} \\ \psi_{g_i s} \end{pmatrix} \tag{4}$$

der u Elemente (2). — Ähnlich entspricht t von G der Substitution

$$\tau = \begin{pmatrix} \psi_{g_i} \\ \psi_{g_i t} \end{pmatrix} \equiv \begin{pmatrix} \psi_{g_i s} \\ \psi_{g_i s t} \end{pmatrix},$$

wo wir also zuletzt in der oberen Reihe die Ordnung (3) der Elemente (2) angenommen haben, was ja nach 70. erlaubt ist. Das Produkt $\sigma\tau$ ersetzt daher ψ_{g_i} durch $\psi_{g_i s t}$ und ist daher gleich einer Substitution vom Typus (4), die aus (4) hervorgeht, wenn s durch st ersetzt wird. Mit anderen Worten: das System aller Substitutionen (4) bildet eine Gruppe Γ. Diese Gruppe ist transitiv, da s als irgendein g_i angenommen werden kann.

Satz 1: Jeder Substitution s von G entspricht eine einzige Substitution σ, die durch (4) definiert ist. Alle solche Substitutioinen σ bilden eine transitive Gruppe Γ.

Wir sahen, daß, wenn t und τ einander entsprechen, dies auch für st und $\sigma\tau$ gilt. Die Korrespondenz zwischen den Substitutionen von G und Γ bleibt also bei der Multiplikation erhalten. G und Γ heißen daher **isomorph.** Je nachdem die Ordnung von G gleich oder größer als die von Γ ist, heißt G einstufig oder mehrstufig isomorph zu Γ. Für einstufig isomorphe Gruppen gelten dieselben Kompositionsregeln; sie sind daher als abstrakte Gruppen identisch.

Beispiel: Ist G die alternierende Gruppe von vier Variabeln, so haben wir

$$G = G_4 + G_4(234) + G_4(243),$$

wo

$$G_4 = \{E, (12)(34), (13)(24), (14)(23)\}.$$

Die angezeigten Substitutionen dritter Ordnung ersetzen $\psi_1 = (x_1 - x_2)(x_3 - x_4)$ durch $\psi_2 = (x_1 - x_3)(x_4 - x_2)$ bzw. $\psi_3 = (x_1 - x_4)(x_2 - x_3)$. Jede Substitution von G_4 läßt ψ_1, ψ_2 und ψ_3 ungeändert. (Vgl. 75., Beisp. 4 und 73., (22)). Daher gehört ψ_1 zu G_4 und hat nur drei Konjugierte unter G. Wir haben also

$$\Gamma = \{E, (\psi_1\psi_2\psi_3), (\psi_1\psi_3\psi_2)\},$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

denn jeder Substitution von G_4 entspricht in Γ die identische Substitution; allen Substitutionen von G_4 (234) entspricht daher dieselbe Substitution $(\psi_1\psi_2\psi_3)$ von Γ. G ist demnach (4, 1) isomorph zu Γ.

Übungen: 1. Wenn G die symmetrische Gruppe und ψ_1 die alternierende Funktion ist, so ist $\Gamma = \{E, (\psi_1\psi_2)\}$.

2. Ist G die symmetrische Gruppe von $x_1, \ldots, x_4$, so ist für

$$y_1 = x_1x_2 + x_3x_4,\ y_2,\ y_3$$

die Gruppe Γ gleich der symmetrischen Gruppe von der Ordnung 6.

3. Wenn G die symmetrische Gruppe von x_1, x_2, x_3 und ψ die sechswertige Funktion $x_1 + \omega^2 x_2 + \omega x_3$ ist, so ist Γ einstufig isomorph zu G (vgl. 69., Beisp. 5).

4. Alle zu H gehörigen Funktionen ψ führen zu derselben Gruppe Γ. — Denn ist φ eine andere zu H gehörige Funktion, so ist es nach 93. eine rationale Funktion $r(\psi)$ von ψ mit Koeffizienten aus K. Wegen Eigenschaft B bleibt $\varphi - r(\psi) = 0$ bei jeder Substitution t von G ungeändert, so daß $\varphi_t = r(\psi_t)$. Daher entspricht irgendeiner Substitution der u Buchstaben (2) dieselbe Substitution der (voneinander verschiedenen) Elemente φ, $\varphi_{g_2}, \ldots \varphi_{g_u}$, und da wir φ und ψ miteinander vertauschen können, so gilt auch das Umgekehrte.

5. Für diese Tatsache, daß Γ einzig durch G und H bestimmt ist und nicht von ψ abhängt, gebe man noch einen anderen Beweis, indem man zeigt, daß die u Komplexe in (1) durch rechtsseitige Multiplikation mit s aus G nur permutiert werden und daß die resultierende Substitution der u Komplexe (abgesehen von der Bezeichnung) dieselbe ist wie die in (4).

101. Die große Wichtigkeit der Gruppe Γ folgt aus dem

Satz 2: Die Resolventengleichung

$$g(y) \equiv (y - \psi_1)(y - \psi_2) \ldots (y - \psi_u) = 0 \tag{5}$$

(wo $\psi_i \equiv \psi_{g_i}$) mit Koeffizienten aus K hat in K die Gruppe Γ.

Um zu beweisen, daß Γ für K die charakteristischen Eigenschaften A und B der Gruppe von (5) hat, beachte man, daß jede rationale Funktion $R(\psi_1, \ldots, \psi_u)$ mit Koeffizienten aus K gleich einer rationalen Funktion $r(x_1, \ldots, x_n)$ mit Koeffizienten aus K ist, so daß die Differenz

$$R(\psi_1, \ldots, \psi_u) - r(x_1, \ldots, x_n) = 0 \tag{6}$$

bei jeder Substitution s der Gruppe G von $x_1, \ldots, x_n$ ungeändert bleibt. Zu s gehört aber eine bestimmte Substitution σ der Gruppe Γ von $\psi_1, \ldots, \psi_u$, so daß

$$R_\sigma(\psi_1, \ldots, \psi_u) - r_s(x_1, \ldots, x_n) = 0. \tag{7}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Nun bleibe zunächst R bei jeder Substitution von Γ ungeändert, so daß $R = R_\sigma$ für jedes in Γ vorkommende σ ist. Durch Vergleichen von (6) und (7) folgt dann, daß auch $r = r_s$ für jedes s ist. Da also r wegen A zu K gehört, so gilt auch für die Gruppe Γ die Eigenschaft A.

Andererseits gehört wegen (6) mit R auch r zu K. Es ist also (wegen B) $r_s = r$ für alle s aus G und damit wegen (6) und (7) auch $R_\sigma = R$ für alle in Γ vorkommenden σ, d. h. Γ hat die Eigenschaft B.

Da endlich Γ transitiv ist, so ist Gleichung (5) in K irreduzibel.

102. Invariante Untergruppen. ψ gehöre zur Untergruppe

$$H = \{h_1 = E, \quad h_2, \ldots, h_p\}$$

von G. Sind dann h und s beliebige Substitutionen aus H bzw. G, so bleibt ψ_s durch Anwendung von $t = s^{-1}hs$ ungeändert, da ψ_s durch s^{-1} in ψ übergeführt wird, ψ durch h ungeändert bleibt und durch s wieder in ψ_s übergeht. — Ist umgekehrt t irgendeine Substitution von G, die ψ_s ungeändert läßt, so daß $\psi_{st} = \psi_s$, so ist

$$\psi_{sts^{-1}} = \psi_{ss^{-1}} = \psi_E = \psi,$$

wo also $sts^{-1} = h$ in H liegt; d. h. es ist $t = s^{-1}hs$. ψ_s gehört demnach zu der Untergruppe

$$\{s^{-1}h_1 s = E, s^{-1}h_2 s, \ldots, s^{-1}h_p s\}$$

von G. Diese Untergruppe bezeichnet man mit $s^{-1}Hs$ und nennt sie die (durch s) Transformierte von H oder eine konjugierte Untergruppe von H. Die Substitution $s^{-1}h_i s$ heißt entsprechend aus h_i durch s transformiert oder zu h_i konjugiert (vgl. 103.). Konjugierte Funktionen gehören also zu konjugierten Untergruppen:

Satz 3: Gehört ψ zur Untergruppe H mit dem Index u unter G, so bilden nach (1) die Funktionen

$$\psi, \psi_{g_2}, \ldots, \psi_{g_u}$$

ein vollständiges System von Konjugierten von ψ unter G. Jede von ihnen gehört zu der entsprechenden konjugierten Gruppe des Systems

$$H, g_2^{-1}Hg_2, \ldots, g_u^{-1}Hg_u.$$

Letzteres System heißt ein (vollständiges) System konjugierter Untergruppen von G. Sind diese alle identisch, so

Digitized by Google Original from UNIVERSITY OF MICHIGAN

heißt H eine invariante[1]) (oder ausgezeichnete) Untergruppe oder ein Normalteiler von G. In diesem wichtigen Falle ist die Substitution (4) die Identität, wenn s in H liegt, da dann jedes ψ_{σ_i} ungeändert bleibt; andererseits entspricht jede Substitution s aus G und das Produkt hs, wo h in H liegt, ein und derselben Substitution (4). Anders ausgedrückt: Betrachten wir die Komplexe $H, Hg_2, \ldots, Hg_u$, welche ja alle Substitutionen von G enthalten, so entsprechen alle Substitutionen von H der identischen Substitution E von Γ; alle Substitutionen von Hg_2 entsprechen ein und derselben Substitution von Γ, usw. Um daher Γ zu erhalten, genügt es, diejenigen Substitutionen herauszugreifen, welche $E, g_2, \ldots, g_u$ entsprechen; denn da sie ψ durch u verschiedene Funktionen ersetzen, so sind auch die resultierenden u Substitutionen von Γ voneinander verschieden. Es gilt daher

Satz 4: Ist H eine invariante Untergruppe von G mit dem Index u, so ist die Gruppe Γ eine transitive Gruppe von der Ordnung u von u Elementen, d. h. eine reguläre Gruppe.

Ist u eine Primzahl und σ eine von E verschiedene Substitution von Γ, so ist die Ordnung von σ gleich u (78., Beisp. 2, 3), so daß Γ durch σ erzeugt werden kann:

Folgerung: Wenn H eine invariante Untergruppe von G vom Primzahlindex u ist, so ist Γ eine reguläre zyklische Gruppe von der Ordnung u.

Diese Folgerung wird durch das Beispiel und die Übung 1 in 100. erläutert, denn beide vorkommenden Untergruppen sind, wie wir im nächsten Paragraphen beweisen werden, invariant in G.

103. Die Transformierten einer Substitution. Es gibt eine einfache Regel, um ohne Ausführung der verlangten Multiplikationen die Transformierte $g^{-1}hg$ von h zu finden. Stellt man nämlich h als Produkt $rst\ldots$ von Zyklen dar, die kein Element gemeinsam haben, so ist offenbar auch

$$g^{-1}hg = g^{-1}rg \cdot g^{-1}sg \ldots,$$

so daß man jetzt nur noch zu wissen braucht, wie ein Zyklus transformiert wird. Ist $r = (abc\ldots e)$,

$$g = \begin{pmatrix} a\,b\,c\ldots e\,f\ldots l \\ A\,B\,C\ldots E\,F\ldots L \end{pmatrix},$$

---

1) Die Invarianz besteht darin, daß H bei allen Substitutionen von G in sich selbst übergeht. — Eine kommutative Gruppe hat lauter invariante Untergruppen.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

also $$g^{-1} = \begin{pmatrix} A\,B\,C \ldots E\,F \ldots L \\ a\,b\,c \ldots e\,f \ldots l \end{pmatrix},$$

so ist $$g^{-1}rg = \begin{pmatrix} A\,B\,C \ldots E\,F \ldots L \\ B\,C\,D \ldots A\,F \ldots L \end{pmatrix} = (A\,B\,C \ldots E);$$

d. h. man erhält $g^{-1}rg$, indem man im Zyklus r die Substitution g ausführt.

Z. B. $(123)^{-1} \cdot (12)(34) \cdot (123) = (23)(14)$. —

Da also jede Substitution ein Produkt von k Transpositionen wieder in ein Produkt von k Transpositionen überführt und daher auch eine grade Substitution wieder in eine grade, so folgt, daß die alternierende Gruppe von u Buchstaben in der symmetrischen Gruppe invariant ist. Der Fall $k = 2$ zeigt dann, daß auch

$$G_4 = \{E, (12)(34), (13)(24), (14)(23)\}$$

invariant unter der symmetrischen Gruppe G_{24} von vier Buchstaben ist, da G_4 jede Substitution der Form $(ab)(cd)$ enthält. —

Eine Substitution heißt in G invariant, wenn sie durch jede Substitution von G in sich selbst transformiert wird.

Übungen: 1. G_4 ist eine invariante Untergruppe der alternierenden Gruppe sowie von G_8, H_8, K_8 (75.).

2. Wenn H eine Untergruppe vom Index 2 ist, so ist H in G invariant. — Denn es ist dann $G = H + Hg = H + gH$, so daß $Hg = gH$, d. h. $H = g^{-1}Hg$.

3. Die einzigen invarianten Substitutionen von G_8 in 75. sind E und $a = (12)(34)$. Daher sind E und $\{E, a\}$ die einzigen invarianten Untergruppen von G_8 von niedrigerer als vierter Ordnung.

104. Einfache Gruppen und Quotientengruppen. Eine Gruppe heißt einfach, wenn sie keine invariante Untergruppe außer E und sich selbst besitzt. Das Gegenteil davon heißt eine zusammengesetzte Gruppe. Z. B. ist jede Gruppe von Primzahlordnung einfach.

H sei eine invariante Untergruppe vom Index u unter G. Nach 93. gibt es eine Funktion ψ, die zu H gehört. Die in 100. definierte Gruppe Γ ist dann von der Ordnung u; sie heißt die Faktorgruppe oder Quotientengruppe von G in bezug auf H und wird mit G/H bezeichnet. Ihre Ordnung u ist der Quotient der Ordnungen von G und H.

Sind z. B. G_6 und G_3 die symmetrische bzw. alternierende Gruppe von 3 Variabeln, so gehört die alternierende Funktion ψ_1 zu G_3, nimmt hingegen in G_6 noch den zweiten Wert $\psi_2 = -\psi_1$ an. G_6/G_3 ist also die Gruppe $\Gamma = \{E, (\psi_1\psi_2)\}$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Eine eigentliche Untergruppe von G ist von G verschieden.

Ist insbesondere H eine größte invariante (eigentliche) Untergruppe (oder ein größter Normalteiler) von G, so daß also H in keinem größeren eigentlichen Normalteiler von G enthalten ist, so gilt der

Satz 5: Die Quotientengruppe $\Gamma = G/H$ ist einfach.

Denn nimmt man an, Γ besitze eine von Γ und E verschiedene invariante Untergruppe $\Delta = \{\alpha_1 = E, \alpha_2, \ldots, \alpha_d\}$, wo α_i allen Substitutionen des Komplexes Ha_i in (1) entspricht, so ist

$$D = Ha_1 + Ha_2 + \cdots + Ha_d, \quad \text{wo} \quad Ha_1 = HE = H,$$

eine Untergruppe von G — da wegen $\alpha_i\alpha_j = \alpha_k$ auch $Ha_i \cdot Ha_j = Ha_k$ — und sogar eine invariante Untergruppe: Denn da jeder Substitution g von G eine Substitution γ von Γ entspricht, so entsprechen wegen der Invarianz von H unter G alle Substitutionen des Komplexes $g^{-1}Ha_ig = H \cdot g^{-1}a_ig$ der Substitution $\alpha_j = \gamma^{-1}\alpha_i\gamma$ der invarianten Untergruppe Δ von Γ, und da die Substitutionen von Ha_j die einzigen sind, die α_j entsprechen, so ist $g^{-1}Ha_ig = Ha_j$, d. h. D ist unter G invariant. Da nun Δ von Γ und E verschieden ist, so ist D von G und H verschieden. H wäre also gegen unsere Voraussetzung in der noch größeren invarianten eigentlichen Untergruppe D von G enthalten.

105. Kompositionsreihen, Primfaktorgruppen, auflösbare Gruppen. Jede Gruppe G enthält die invariante Gruppe E. Da G endlich ist, so ist es auch die Zahl seiner Untergruppen. Jede Gruppe besitzt daher eine größte invariante Untergruppe G_1. Ähnlich besitzt G_1 eine größte invariante Untergruppe G_2, usw. Eine solche mit E schließende Reihe von Untergruppen $G, G_1, G_2, \ldots, G_m, E$ heißt eine Kompositionsreihe von G. G/G_1, G_1/G_2, $G_2/G_3, \ldots,$ $G_m/E = G_m$ heißen die Primfaktorgruppen von G [in bezug auf die Kompositionsreihe[1]) $G, G_1, \ldots, E$]; ihre Ordnungen bilden die Indexreihe von G (in bezug auf $G, G_1, G_2, \ldots, E$).

---

1) In Wirklichkeit sind, wie Jordan und Hölder bewiesen, für alle Kompositionsreihen die Primfaktorgruppen von G (abgesehen von der Anordnung) dieselben. Vgl. Jordan, Traité des Substitutions, 1870, p. 42, wo allerdings nur die Gleichheit der Indexreihen bewiesen wird; Hölder, Math. Ann. 34, 1889, p. 37; Miller, Blichfeldt and Dickson, Theory and Application of Finite Groups, 1916, p. 175; Speiser, Gruppentheorie, Berlin 1923, p. 22.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Eine Gruppe heißt auflösbar, wenn ihre Indexreihe aus lauter Primzahlen besteht. Die Primfaktorgruppen sind in diesem Falle alle einfach und zyklisch.

Übungen: 1. Sind G_6 und G_3 die symmetrische bzw. alternierende Gruppe von drei Buchstaben, so ist G_6, G_3, E die einzige Kompositionsreihe von G_6; G_6 ist auflösbar.

2. Eine (zyklische) Gruppe von Primzahlordnung ist auflösbar. — Denn ihre Kompositionsreihe ist G, E.

3. Die symmetrische Gruppe von vier Buchstaben hat die Kompositionsreihe G_{24}, G_{12} = altern. Gruppe, G_4 (in 100., Beisp.), G_2, E, wo für G_2 drei Möglichkeiten bestehen. G_{24} ist demnach auflösbar.

4. Wenn C_{12} durch $a = (x_1 x_2 \ldots x_{12})$ erzeugt wird, so sind die einzigen eigentlichen Untergruppen

$$C_6 = \{E, a^2, a^4, a^6, a^8, a^{10}\}, \quad C_4 = \{E, a^3, a^6, a^9\},$$
$$C_3 = \{E, a^4, a^8\}, \quad C_2 = \{E, a^6\} \text{ und } C_1 = E.$$

Da jede Untergruppe einer kommutativen Gruppe invariant ist, so sind

$$C_{12}, C_6, C_3, E; \quad C_{12}, C_6, C_2, E; \quad C_{12}, C_4, C_2, E$$

die einzigen Kompositionsreihen von C_{12}. Die Indexreihen sind 2, 2, 3; 2, 3, 2; 3, 2, 2, unterscheiden sich also in der Tat nur durch die Anordnung.

5. Wenn G eine Untergruppe H vom Index 2, H wieder eine Untergruppe K vom Index 2 hat, usw. bis zu E, so ist $G, H, K, \ldots, E$ eine Kompositionsreihe von G (vgl. 103., Übg. 2).

6. Man finde die sieben Kompositionsreihen von G_8 in 75.

7. Man beweise, daß die drei Kompositionsreihen von Beispiel 3 die einzigen sind.

106. Satz 6: Die Lösung einer Gleichung mit der Gruppe G für für den Bereich K läßt sich zurückführen auf die Lösung einer Kette von Gleichungen. Jede dieser Gleichungen besitzt in dem Bereich, den man bekommt, wenn man zu K eine Wurzel jeder der früheren Gleichungen der Kette adjungiert, eine einfache reguläre Gruppe. Ist insbesondere G auflösbar, so hat jede Hilfsgleichung eine reguläre zyklische Gruppe von Primzahlordnung.

$G, G_1, G_2, \ldots, E$ sei eine Kompositionsreihe von G und $n_1, n_2, \ldots$ sei ihre Indexreihe. Man baue eine rationale Funktion ψ der Wurzeln x_i mit Koeffizienten aus K, die zur Untergruppe G_1 von G mit dem Index n_1 gehört (93.). Dann ist ψ die Wurzel einer Gleichung vom Grade n_1 mit Koeffizienten aus K, deren Gruppe Γ für K einstufig isomorph ist zu der einfachen Faktorgruppe G/G_1 (101.,

Digitized by Google Original from UNIVERSITY OF MICHIGAN

104.). Nach Adjunktion von ψ zu K reduziert sich nach 94. die Gruppe der Gleichung für den Körper $K(\psi)$ auf G_1.

Sodann suche man eine rationale Funktion χ der x_i mit Koeffizienten aus $K(\psi)$, die zur Untergruppe G_2 von G_1 vom Index n_2 gehört. Dann ist χ eine Wurzel einer Gleichung vom Grade n_2 mit Koeffizienten aus $K(\psi)$, deren Gruppe für diesen Bereich einstufig isomorph ist mit der einfachen Gruppe G_1/G_2. Nach Adjunktion von χ reduziert sich für den Bereich $K(\psi, \chi)$ die Gruppe der gegebenen Gleichung auf G_2. Usw.

Schließlich wird man zur Adjunktion einer zu E gehörenden Funktion geführt. Der so entstandene erweiterte Bereich enthält dann jedes x_i.

Folgerung: Damit — ausgehend vom Bereich K — eine Gleichung sich auf eine Kette von Hilfsgleichungen von den Gradzahlen $n_1, n_2, \ldots$ zurückführen läßt, ist notwendig (aber natürlich nicht hinreichend!), daß die Ordnung ihrer Gruppe für K gleich dem Produkt $n_1 \cdot n_2 \cdot n_3 \cdots$ der Grade der Hilfsgleichungen ist. Sind insbesondere die $n_1, n_2, \ldots$ alles Primzahlen, so läßt sich die Gleichungskette nicht durch eine solche mit niedrigeren Gradzahlen ersetzen.

107. Zyklische Gleichungen. Der Satz 6 findet seine Ergänzung in

Satz 7: Wenn für einen Körper K, der eine imaginäre $p$te Einheitswurzel ϱ enthält, eine Gleichung eine reguläre zyklische Gruppe von der Primzahlordnung p besitzt, so ist die Gleichung in K auflösbar.

Die Wurzeln seien $x_0, x_1, \ldots, x_{p-1}$; $s = (x_0 x_1 \ldots x_{p-1})$ sei eine Erzeugende von G, so daß alle Substitutionen von G Potenzen von s sind. Offenbar wird

$$r_i = x_0 + \varrho^i x_1 + \varrho^{2i} x_2 + \cdots + \varrho^{(p-1)i} x_{p-1}, \qquad (i = 0, \ldots, p-1) \tag{8}$$

durch s in $\varrho^{-i} r_i$ übergeführt. $v_i = r_i^p$ bleibt daher durch s ungeändert. Da die Koeffizienten von v_i zu K gehören und da v_i gegenüber allen Substitutionen s^k von G sich invariant verhält, so ist es (nach 91. A.) eine Größe aus K. Die p linearen Gleichungen (8) für $i = 0, \ldots, p-1$ können nach den p Unbekannten $x_0, x_1, \ldots, x_{p-1}$ aufgelöst werden, wie es in 68. für den Fall $n = 3$ geschehen ist. Multipliziert man nämlich (8) mit ϱ^{-ij}, wo $0 \leqq j < p$, und summiert von $i = 0$ bis $i = p-1$, so ist in der

Digitized by Google Original from UNIVERSITY OF MICHIGAN

entstehenden Gleichung der Koeffizient von x_j gleich $1 + 1 + \cdots + 1 = p$, während man für $k \neq j$ als Koeffizienten von x_k

$$\sum_{i=0}^{p-1} \varrho^{ti} = \frac{\varrho^{tp} - 1}{\varrho^t - 1} \qquad (\text{wo } t = k - j),$$

also Null bekommt, da t nicht durch p teilbar ist. Also ist[1])

$$p x_j = r_0 + \sum_{i=1}^{p-1} \varrho^{-ij} v^{\frac{1}{p}} \qquad (j = 0, 1, \ldots, p-1),$$

wo $-r_0$ ein Koeffizient der gegebenen Gleichung ist, also in K liegt. Eine solche Gleichung, deren Gruppe zyklisch ist, heißt selbst zyklisch.

108. Kreisteilungsgleichungen. Der letzte Satz zeigte, daß gewisse Gleichungen nach Adjunktion einer Einheitswurzel auflösbar werden. Um ihn zu vervollständigen, wollen wir nunmehr beweisen, daß auch die $p$ten Einheitswurzeln, wenn p eine ungrade Primzahl ist, selbst wieder durch Wurzelziehen gefunden werden können. Diese Wurzeln sind die sukzessiven Potenzen einer von ihnen, etwa von ϱ. Für $p = 5$ können wir sie in die Anordnung

$$\varrho, \varrho^2, \varrho^{2^2} = \varrho^4, \varrho^{4^2} = \varrho^3$$

bringen, wo also jede Potenz das Quadrat der vorhergehenden ist.

Im übrigen können wir, ohne daß die Untersuchung dadurch schwieriger würde, statt der $p$ten sofort die p^sten Einheitswurzeln suchen; dadurch bekommen wir zugleich Resultate, die uns bei unserem späteren Studium der regulären Polygone von Nutzen sind.

In 85. sahen wir nun z. B., daß die primitiven neunten Einheitswurzeln gleich

$$\varrho, \varrho^2, \varrho^4, \varrho^8, \varrho^{16} = \varrho^7, \varrho^{32} = \varrho^5$$

sind, wo wiederum jede das Quadrat der vorhergehenden ist; ferner, daß die $e = p^s - p^{s-1}$ primitiven p^sten Einheitswurzeln Potenzen einer von ihnen, etwa von ϱ, sind, deren Exponenten die positiven ganzen, durch p nicht teilbaren Zahlen $< p^s$ sind. Die obigen, sich auf die Fälle $p = 5$, $p^2 = 9$ beziehenden Tatsachen lassen sich verallgemeinern: In der Zahlentheorie wird nämlich

1) Lagrange, Traité d. résolution d. équations, 1808, XIII, § 16. — Nouv. Mém. Acad. Berlin, 1770, § 71; Œuvres III, p. 333.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

gezeigt, daß es zu p^s eine ganze Zahl gibt g von der Beschaffenheit, daß die Reste von $1, g, g^2, \ldots, g^{e-1}$ nach p^s abgesehen von der Anordnung mit den Zahlen übereinstimmen, die kleiner als p^s und nicht teilbar durch p sind. Sie geben daher die erwähnten Exponenten von ϱ. Daraus folgt, daß die primitiven p^sten Einheitswurzeln

$$x_1 = \varrho, \quad x_2 = \varrho^g, \quad x_3 = \varrho^{g^2}, \ldots, x_e = \varrho^{g^{e-1}}$$

sind, d. h. es ist

$$(9) \qquad x_2 = x_1^g, \quad x_3 = x_2^g, \ldots, x_e = x_{e-1}^g, \quad x_1 = x_e^g.$$

Die letzte dieser Beziehungen ergibt sich aus dem Eulerschen Satz der Zahlentheorie, daß g^e auf die Form $1 + k \cdot p^s$, wo k ganzzahlig ist, gebracht werden kann. — Man vergleiche hiermit die obigen Fälle $p^s = 5$, $p^s = 9$.

In 85. bewiesen wir nun, daß diese Gleichung mit den Wurzeln $x_1, \ldots, x_e$ in R irreduzibel ist. Ihre Gruppe ist daher für R transitiv. Ist jetzt

$$s = \begin{pmatrix} x_1 x_2 x_3 \ldots x_e \\ x_a x_b x_c \ldots x_l \end{pmatrix}$$

eine Substitution aus G, so folgt aus (9) wegen Eigenschaft B, daß

$$x_b = x_a^g, \quad x_c = x_b^g, \ldots, \quad x_a = x_l^g.$$

Nun ist andererseits nach (9) $x_{a+1} = x_a^g$ usw., also auch

$$x_b = x_{a+1}, \quad x_c = x_{b+1}, \ldots, \quad x_a = x_{l+1}.$$

(Dabei wird x_{e+1} durch x_1 ersetzt.) Unterscheiden sich zwei ganze Zahlen u und v nur durch ein Vielfaches von e, so schreibt man: $u \equiv v \pmod{e}$. Danach ist

$$b \equiv a + 1, \quad c \equiv b + 1 \equiv a + 2, \ldots \pmod{e},$$

also

$$s = \begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_k & \ldots & x_e \\ x_a & x_{a+1} & x_{a+2} & \ldots & x_{k+a-1} & \ldots & x_{e+a-1} \end{pmatrix},$$

wo wiederum x_{e+j} durch x_j ersetzt wird. Es ist demnach

$$s = t^{a-1} = (x_1 x_2 x_3 \ldots x_e)^{a-1}.$$

Und da G transitiv ist, so enthält es sämtliche Potenzen von t.

Satz 8: Ist p ein ungrade Primzahl, so ist in R die Gruppe der Kreisteilungsgleichung, deren Wurzeln die primitiven p^sten Einheitswurzeln sind, eine reguläre zyklische Gruppe von der Ordnung $e = p^s - p^{s-1}$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Für den Fall $p^s = 5$ hatten wir den Satz in 92., Beispiel 8 bestätigt.

109. Die hinreichende Bedingung für die Lösbarkeit durch Radikale. Eine Gleichung, deren Gruppe in dem Bereich ihrer Koeffizienten auflösbar ist, ist selbst auflösbar, d. h. durch Radikale lösbar. — Allgemeiner gilt

Satz 9: Eine Gleichung, die für irgendeinen, die Koeffizienten enthaltenden Bereich K eine auflösbare Gruppe besitzt, ist in K auflösbar.

Man setze zunächst den Satz als gültig voraus für jede Gleichung, die für K eine reguläre zyklische Gruppe von Primzahlordnung besitzt. — Nach 106. gibt es eine Gleichungskette $F_1(\psi) = 0$, $F_2(\chi) = 0, \ldots$ von den Primzahlgraden $n_1, n_2, \ldots$, deren Lösung der Lösung von $f(x) = 0$ äquivalent ist. Wie dort bewiesen wurde, ist für K die Gruppe von $F_1(\psi) = 0$ eine reguläre zyklische Gruppe von der Primzahlordnung n_1, die unserer Voraussetzung nach bezüglich K auflösbar ist. Die Koeffizienten von $F_2(\chi) = 0$ gehören zu dem Körper $K_1 = K(\psi)$, und die Gruppe von $F_2(\chi) = 0$ bezüglich K_1 ist eine reguläre zyklische Gruppe von der Primzahlordnung n_2 (106.), also bezüglich K_1 auflösbar und daher auch in bezug auf K, da wir soeben für $F_1(\psi) = 0$ die Auflösbarkeit bewiesen hatten. — Ähnlich sind alle unsere Hilfsgleichungen bezüglich K auflösbar. Und da die Wurzeln von $f(x) = 0$ rational durch Größen aus K und durch die Wurzeln $\psi, \chi, \ldots$ dieser Hilfsgleichungen ausdrückbar sind, so ist $f(x) = 0$ selbst in K auflösbar.

Es ist jetzt noch unsere obige Voraussetzung zu beweisen, daß jede Gleichung $C(x) = 0$ mit einer regulären zyklischen Gruppe von der Primzahlordnung p bezüglich K durch Radikale mit dem Index $\leqq p$ lösbar ist. Der Satz ist offenbar für $p = 2$ richtig, da wir dann eine quadratische Gleichung vor uns haben; um ihn durch Induktion zu beweisen, nehmen wir ihn für alle Primzahlen $< p$ als richtig an. Nach dem vorhergehenden Paragraphen folgt daraus, daß auch die Gleichung für die imaginären $p$ten Einheitswurzeln bezüglich R durch Radikale mit kleinerem als $p$tem Index lösbar ist. In der Tat ist ihre Gruppe für R eine reguläre zyklische von der Ordnung $p-1$, deren Indexreihe aus Primfaktoren von $p-1$ besteht, also aus Primzahlen, die kleiner als p sind.

Adjungiert man jetzt zu K eine imaginäre $p$te Einheitswurzel ϱ, so ist in $K(\varrho)$ die Gruppe von $C(x) = 0$ entweder die Ausgangsgruppe G oder die Einheitsgruppe E (94.). Im letzteren Fall

Digitized by Google Original from UNIVERSITY OF MICHIGAN

liegen die Wurzeln in $K(\varrho)$ und können daher aus Größen aus K rational und durch Wurzeloperationen vom Index $< p$ gefunden werden, denn auch ϱ läßt sich ja aus rationalen Zahlen durch diese Operationen ableiten. Dann ist also $C(x) = 0$ bezüglich K durch Radikale von kleinerem als $p$tem Index lösbar. — Im ersteren Fall ist nach 107. die Gleichung $C(x) = 0$ bezüglich $K(\varrho)$ und also auch bezüglich K durch Radikale mit den Indizes $\leqq p$ lösbar. — Damit ist unser Satz vollständig bewiesen.

Folgerung: Ist p eine ungrade Primzahl, so ist die Gleichung der $p-1$ imaginären $p$ten Einheitswurzeln durch Radikale von kleinerem als $p$tem Index lösbar.

Beispiel 1: Wenn b, c, d unabhängige Variabeln sind und ω eine imaginäre dritte Einheitswurzel ist, so ist für den Körper $R(\omega, b, c, d)$ die Gruppe von $x^3 + bx^2 + cx + d = 0$ die symmetrische Gruppe der drei Wurzeln (95.). Da diese nach 105., Beispiel 1 auflösbar ist, so ist es auch die Gleichung (99.). Nach Adjunktion der Quadratwurzel aus der Diskriminante besitzt die Gleichung eine zyklische Gruppe dritter Ordnung.

Beispiel 2: Man betrachte eine Gleichung vierten Grades, deren Koeffizienten unabhängige Variabeln sind. In dem Körper K ihrer Koeffizienten ist ihre Gruppe die symmetrische Gruppe G_{24} der Wurzeln. Sie ist nach 105., Beispiel 3 auflösbar. Zu der invarianten Untergruppe G_{12}, die aus allen graden Substitutionen besteht, gehört das Produkt P der Wurzeldifferenzen. Das Quadrat von P ist gleich der Diskriminante der Ausgangsgleichung. Im Körper $K_1 = K(P)$ reduziert sich die Galoissche Gruppe auf G_{12}. — Die Funktion $y_1 = x_1x_2 + x_3x_4$ bleibt durch $G_4 = \{E, (12)(34), (13)(24), (14)(23)\}$ ungeändert, geht jedoch durch die übrigen acht Substitutionen von G_{12} in y_2 bzw. y_3 über. Nach 93. sind y_1, y_2, y_3 die Wurzeln einer kubischen Gleichung mit Koeffizienten aus K_1, nämlich der kubischen Resolvente von 73. Da G_4 in G_{12} invariant ist, so ist für den Körper $K(P)$ die Gruppe dieser Resolvente gleich G_{12}/G_4 also zyklisch und von dritter Ordnung. Durch Adjunktion von y_1 zu K_1 reduziert sich die Gruppe der biquadratischen Gleichung auf G_4. — Ferner bleibt x_1x_2 durch $G_2 = \{E, (12)(34)\}$ ungeändert, während die übrigen Substitutionen von G_4 es in x_3x_4 überführen. Die Adjunktion einer Wurzel von $z^2 - y_1z + x_1x_2x_3x_4 = 0$ erniedrigt daher die Gruppe der Gleichung von G_4 auf die invariante Untergruppe G_2. Schließlich wird G_2 durch Adjunktion von $x_1 - x_2$, dessen Quadrat zu $K_1(y_1, x_1x_2)$ gehört, auf E reduziert. Der erweiterte Körper enthält dann x_1, x_2, x_3, x_4. — Die Lösung der Gleichung erfordert demnach das Ausziehen von drei Quadratwurzeln und einer Kubikwurzel.

Übungen: 1. An Stelle von y_1 in Beispiel 2 können wir auch

$$t_1^2 = 4y_1 + b^2 - 4c, \text{ wo } t_1 \equiv x_1 + x_2 - x_3 - x_4$$

ist, verwenden (vgl. 75., Beisp. 3). Offenbar ersetzt die Transformation $y = \frac{1}{4}(t^2 - b^2 + 4c)$ die frühere kubische Resolvente durch eine solche in t,

Digitized by Google Original from UNIVERSITY OF MICHIGAN

deren Wurzeln die Quadrate von $t_1, t_2 = x_1 + x_3 - x_2 - x_4$ und $t_3 = x_1 + x_4 - x_2 - x_3$ sind. Die Wurzeln x_i bestimmen sich dann aus diesen drei linearen Gleichungen und aus $-b = \sum x_1$.

2. In Beispiel 2 adjungiere man zu dem Stammkörper die kubische Einheitswurzel ω und verwende statt y_1 die Funktion $\varphi = y_1 + \omega y_2 + \omega^2 y_3$. Setzt man dann $\psi = y_1 + \omega^2 y_2 + \omega y_3$, so ergibt sich, wenn man die Ergebnisse (6) und (7) von 68. auf die kubische Resolvente (19) von 73. anwendet, daß

$$\varphi^3 - \psi^3 = 3(\omega - \omega^2) P, \quad \varphi\psi = c^2 - 3bd + 12e,$$
$$\varphi^3 + \psi^3 = 2c^3 - 9bcd - 72ce + 27d^2 + 27b^2 e,$$

wo also im wesentlichen die Invarianten I und J von 12. auftreten. φ ergibt sich dann durch Ausziehen einer dritten Wurzel, so daß jetzt auch ψ bekannt ist. Aus den Werten von φ, ψ und $y_1 + y_2 + y_3 = c$ erhält man y_1, y_2, y_3 durch Lösung dreier linearer Gleichungen (vgl. 68.). In $K_1 = K(P, \varphi)$ ist dann G_4 die Gruppe der biquadratischen Gleichung. Wird jetzt noch die Wurzel t_1 von $t_1^2 = 4y_1 + b^2 - 4c$ adjungiert, so erniedrigt sich die Gruppe auf $G_2 = \{E, (12)(34)\}$. Schließlich erhält man durch Adjunktion der Wurzel t_2 von $t_2^2 = 4y_2 + b^2 - 4c$ die identische Gruppe E, und die x ergeben sich wie in Übung 1, wobei man noch beachte, daß $t_1 t_2 t_3 = 4bc - b^3 - 8d$. — Durch die alleinige Verwendung zweigliedriger Resolventen und die Einführung der Invarianten I und J wird diese Lösung besonders elegant.

110. Der Jordansche[1]) Satz über die gegenseitige Adjunktion von Wurzeln.

Satz 10: Erniedrigt sich für den Bereich K die Gruppe G_1 einer algebraischen Gleichung $f_1(x) = 0$ durch Adjunktion aller Wurzeln einer zweiten Gleichung $f_2(x) = 0$ auf H_1 und erniedrigt sich umgekehrt die Gruppe der zweiten Gleichung durch Adjunktion aller Wurzeln der ersten Gleichung auf H_2, so sind H_1 und H_2 invariante Untergruppen von G_1 bzw. G_2 vom gleichen Index und[2]) die Quotientengruppen G_1/H_1 und G_2/H_2 sind zueinander einstufig isomorph.

Nach 93. gibt es eine rationale Funktion g_1 der Wurzeln $x_1, \ldots, x_n$ der ersten Gleichung mit Koeffizienten aus K, die zur Untergruppe H_1 von G_1 gehört. Da sich durch die Adjunktion der

---

1) Traité des Subsitutions, 1870, pp. 268f.

2) Diesen Zusatz verdankt man Hölder, Math. Ann. 34, 1889, p. 47. Betr. Verallgemeinerungen und weiterer Ergebnisse vergleiche man Kneser, ibid. 30, 1887, pp. 179—202; ein kürzerer Beweis des Satzes (ibid. p. 195) findet sich in Journ. f. Math. 106, 1890, p. 51. — Landsberg, ibid. 132, 1907, pp. 1—20. — Bucca, Rendic. Circ. Mat. Palermo 14, 1900, pp. 122—126. — Loewy, Math. Zeitschrift 15, 1922, pp. 261—273.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Wurzeln $y_1, \ldots, y_m$ der zweiten Gleichung G_1 auf H_1 reduziert, so ist (91., A.) g_1 eine Größe des erweiterten Bereiches, d. h. es ist

$$g_1(x_1, \ldots, x_n) = h_1(y_1, \ldots, y_m), \tag{10}$$

wo h_1 eine rationale Funktion mit Koeffizienten aus K bezeichnet. Sind $g_1, \ldots, g_k$ die Konjugierten von g_1 unter G_1, so ist k der Index von H_1 unter G_1 (93.). Umgekehrt mögen $h_1, \ldots, h_l$ die Konjugierten von h_1 unter G_2 bezeichnen. Diese k Funktionen g_i bzw. l Funktionen h_i sind die Wurzeln je einer in K irreduziblen Gleichung vom Grade k bzw. l. Da indessen diese beiden Gleichungen eine Wurzel (10) gemeinsam haben, so sind sie nach 82. identisch. Es ist also $k = l$ und die g sind abgesehen von der Anordnung gleich den h.

Ist jetzt s_i eine Substitution aus G_1, die g_1 durch g_i ersetzt, so transformiert s_i die Gruppe H_1, zu der g_1 gehört, in die Gruppe H_i, zu der g_i gehört (102.). Da aber g_i gleich einem gewissen h_j ist und daher in $K' = K(y_1, \ldots, y_m)$ liegt, so verhält es sich gegenüber H_1, welches ja für den Bereich K' die Gruppe von $f_1(x) = 0$ ist, invariant. Daher enthält die Gruppe H_i, zu der g_i gehört, alle Substitutionen von H_1 und fällt, da sie von derselben Ordnung wie H_1 ist, mit H_1 zusammen, d. h. H_1 ist invariant unter G_1. Nach 104. ist dann für K die Gruppe der irreduziblen Gleichung, der g_1 genügt, die Quotientengruppe G_1/H_1.

I sei nunmehr die Untergruppe von G_2, zu der $h_1(y_1, \ldots, y_m)$ gehört. Sie ist vom Index k, da h_1 die Wurzel einer in K irreduziblen Gleichung vom Grade k ist. Durch Adjunktion von h_1 oder, was nach (10) dasselbe ist, von g_1 erniedrigt sich die Gruppe G_2 von $f_2(x) = 0$ auf I (94.). Wird nicht nur $g_1(x_1, \ldots, x_n)$, sondern werden sogar alle x_i selbst adjungiert, so reduziert sich G_2 auf eine Untergruppe von I. H_2 ist also in I enthalten. — Damit haben wir als vorläufiges Ergebnis: Wenn sich die Gruppe von $f_1(x) = 0$ durch Adjunktion aller Wurzeln von $f_2(x) = 0$ auf eine Untergruppe vom Index k reduziert, so reduziert sich durch Adjunktion aller Wurzeln von $f_1(x) = 0$ die Gruppe von $f_2(x) = 0$ auf eine Untergruppe vom Index $k_1 \geqq k$. — Vertauscht man in diesem Satz $f_2(x)$ mit $f_1(x)$, so folgt leicht, daß $k = k_1$ ist. Da nun H_2 in I enthalten und vom Index k_1 unter G_2 und da I vom Index k unter G_2 ist, so sind H_2 und I identisch.

Ebenso wie H_1 in G_1 so ist natürlich auch H_2 in G_2 invariant. Ebenso ist $G_2/I = G_2/H_2$ für K die Gruppe der irreduziblen Gleichung, der h_1 genügt. Da diese Gleichung aber mit derjenigen

Digitized by Google Original from UNIVERSITY OF MICHIGAN

von g_1 identisch ist und da die Gruppe der letzteren Gleichung gleich G_1/H_1 ist, so unterscheiden sich G_1/H_1 und G_2/H_2 nur in der Bezeichnung der Elemente, auf die sie sich beziehen, d. h. sie sind einstufig isomorph.

111. Der Galoissche Satz über die Adjunktion von Wurzeln.

Satz 11: Ist $f_2(x) = 0$ eine Gleichung, die für K eine reguläre zyklische Gruppe von der Primzahlordnung p besitzt, so erniedrigt sich durch Adjunktion einer ihrer Wurzeln die Gruppe G_1 der Gleichung $f_1(x) = 0$ entweder auf eine invariante Untergruppe H_1 vom Index p oder sie bleibt ungeändert.

Dies ist eine einfache Folgerung des Jordanschen Satzes, da man mit der Adjunktion einer Wurzel x_1 von $f_2(x) = 0$ in Wirklichkeit alle ihre Wurzeln adjungiert. Denn die einzige Substitution der (regulären) Gruppe von $f_2(x) = 0$ für den Bereich K, welche x_1 ungeändert läßt, ist E, so daß jede Wurzel eine rationale Funktion von x_1 mit Koeffizienten aus K ist (93., Satz 10), d. h. zu $K(x_1)$ gehört.

Es ist also dann G_1/H_1 isomorph zu G_2/H_2. Letztere aber ist entweder gleich E oder gleich G_2, weil G_2 einfach ist; d. h. es ist entweder $H_1 = G_1$ oder H_1 vom Index p unter G_1.

112. Das Galoissche Kriterium für die Auflösbarkeit. Damit eine algebraische Gleichung auflösbar ist, ist notwendig und hinreichend, daß ihre Gruppe im Bereich ihrer Koeffizienten auflösbar ist.

Dieser Satz kann, was oft von Nutzen ist, in der verallgemeinerten Form ausgesprochen werden:

Satz 12: Damit eine Gleichung in einem Bereich K, der ihre Koeffizienten enthält, auflösbar ist, ist notwendig und hinreichend, daß ihre Gruppe für K auflösbar ist.

Daß diese Bedingung hinreicht, wurde in 109. bewiesen. Wir brauchen daher jetzt nur zu beweisen, daß sie notwendig ist. Wir nehmen also an, daß die Wurzeln $x_1, \ldots, x_n$ sich rational und durch Wurzeloperationen aus Größen aus K oder aus Größen, die sich aus ihnen durch solche Operationen ergeben, bestimmen lassen. Der Index jeder Wurzel kann natürlich als Primzahl angenommen werden, da eine pqte Wurzel die $p$te Wurzel einer $q$ten Wurzel ist. Ein Verzeichnis aller Radikale

$$a_1^{\frac{1}{p_1}}, \quad a_2^{\frac{1}{p_2}}, \ldots, \quad a_k^{\frac{1}{p_k}}, \tag{11}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

die in den Ausdrücken für $x_1, \ldots, x_n$ vorkommen, ist so anzulegen, daß a_1 in K liegt, a_2 in dem durch Adjunktion des ersten Radikals zu K erweiterten Bereich, a_3 in dem durch Adjunktion der beiden ersten Radikale zu K erweiteretn Bereich, usw. Die $p_1, \ldots, p_k$ sind dann ebenfalls Primzahlen.

Nach der Folgerung aus 109. ist die Gleichung für die imaginären $p$ten Einheitswurzeln (wo p eine Primzahl ist) durch Radikale mit kleinerem als $p$tem Index lösbar. Daher lassen sich diese Wurzeln rational durch Radikale, die eine Kette vom Typus (11) bilden, ausdrücken, nur tritt an Stelle von K der Bereich der rationalen Zahlen. Man schreibe die Radikale der Kette für $p = 3$ nieder, dann die für $p = 5$, überhaupt die für alle Primzahlen bis zur größten Primzahl von $p_1, \ldots, p_k$ (diese selbst eingeschlossen). Hinter das letzte dieser Radikale schreibe man die Radikale (11) in geordneter Reihenfolge. So bekommen wir eine Kette von Radikalen

$$b_1^{\frac{1}{q_1}}, \quad b_2^{\frac{1}{q_2}}, \ldots, \quad b_s^{\frac{1}{q_s}} \tag{12}$$

mit folgenden Eigenschaften: Die $q_1, \ldots, q_s$ sind Primzahlen. Sodann liegt b_1 in K, b_2 bzw. b_3 usw. jedoch liegen in denjenigen Bereichen, die aus K durch Adjunktion des ersten Radikals bzw. der beiden ersten Radikale usw. entstehen. Drittens sind $x_1, \ldots, x_n$ rationale Funktionen dieser Radikale mit Koeffizienten aus K, die sie ja auch solche Funktionen der miteinbegriffenen Radikale (11) waren. Viertens erhalten wir nach Adjunktion der ersten $r - 1$ Radikale (12) zu K einen Körper, der alle $q_r$ten Einheitswurzeln enthält.

Jetzt brauchen wir folgenden

Hilfssatz: Für einen Bereich, der A und eine imaginäre p-te Einheitswurzel ϱ (wo p eine Primzahl $\neq 2$) enthält, ist die Gruppe von $x^p = A$ die identische, wenn eine ihrer Wurzeln zu dem Bereich gehört; ist jedoch keine Wurzel in dem Bereich enthalten, so ist die Gruppe zyklisch und regulär und von der Ordnung p.

Denn ist r eine Wurzel dieser Gleichung, so sind die übrigen Wurzeln gleich $r, \varrho r, \ldots, \varrho^{p-1} r$. Enthält der Körper, der ϱ enthält, auch r, so gehören alle diese Wurzeln zu ihm. Die Gruppe ist in diesem Falle gleich E. — Gehört aber keine Wurzel zu dem Körper, ist also A nicht die $p$te Potenz einer Zahl des Körpers, so ist nach 84. $x^p - A$ irreduzibel, die Gruppe also transitiv und

Digitized by Google Original from UNIVERSITY OF MICHIGAN

daher von der Ordnung $\geqq p$. Bei entsprechender Numerierung der Wurzeln x_i ist

$$x_2 = \varrho x_1,\ x_3 = \varrho x_2, \ldots, x_p = \varrho x_{p-1},\ x_1 = \varrho x_p.$$

Ist jetzt $$s = \begin{pmatrix} x_1 x_2 x_3 \cdots x_p \\ x_a x_b x_c \cdots x_e \end{pmatrix}$$

eine Substitution der Gruppe, so ist wegen 91. B

$$x_b = \varrho x_a = x_{a+1},\quad x_c = \varrho x_b = x_{b+1}, \ldots$$

Wie in 108. ist daher $s = (x_1 x_2 \ldots x_p)^{a-1}$, wo $(x_1 \ldots x_p)$ eine Erzeugende der Gruppe ist. Die Gruppe hat also die Ordnung p. —

Nun sei im Bereich K die Gruppe der gegebenen Gleichung mit den Wurzeln $x_1, \ldots, x_n$ gleich G. Adjungiert man jetzt zu K das erste der Radikale (12), welches ja der Gleichung $x^{q_1} = b_1$ genügt, so wird nach unserem Hilfssatz und nach dem Galoisschen Satz von 111. die Gruppe G entweder überhaupt nicht reduziert oder auf eine invariante Untergruppe vom Index q_1 reduziert. Die jetzt folgende Adjunktion des zweiten Radikals (12) läßt die neue Gruppe entweder stehen oder erniedrigt sie auf eine invariante Untergruppe vom Index q_2. Durch die sukzessive Adjunktion aller Radikale (12) bekommt man schließlich einen $x_1, \ldots, x_n$ enthaltenden Körper, für den die Gruppe gleich E ist. Da wir von G zu E über eine Reihe von Untergruppen gelangten, deren jede in der vorhergehenden invariant und vom Primzahlindex war, so haben wir eine Kompositionsreihe von G vor uns, deren Indexreihe aus lauter Primzahlen besteht, d. h. G ist auflösbar.

113. Die Nichtauflösbarkeit der allgemeinen Gleichung vom Grade $n > 4$. Nach 95. ist die Gruppe der allgemeinen Gleichung (d. h. deren Koeffizienten unabhängige komplexe Variablen sind) vom Grade n für den Körper, der durch die Koeffizienten und durch endlich viele Konstante bestimmt ist, die symmetrische Gruppe G. Diese hat (103.) immer eine invariante Untergruppe, die alternierende Gruppe. Von letzterer gilt nun der wichtige

Satz 13: Die alternierende Gruppe von mehr als vier Elementen ist einfach.

Denn angenommen, die alternierende Gruppe A besitze eine von E verschiedene invariante Untergruppe H. Aus den Substitutionen von H, mit Ausnahme von E, greife man diejenigen

Digitized by Google Original from UNIVERSITY OF MICHIGAN

heraus, die sich auf die geringste Zahl von Elementen beziehen. Alle in einer solchen Substitution h vorkommenden Zyklen enthalten gleich viel Elemente. Denn wenn h zwei Zyklen mit a bzw. b Elementen enthält, wo $a < b$ ist, so ist $h^a \neq E$ und berührt, da es die a Elemente ungeändert läßt, weniger Elemente als h selbst, und dies widerspricht der vorausgesetzten Eigenschaft von h.

Da H invariant in A sein soll, so enthält es jede durch irgendeine grade Substitution e Transformierte von h, also auch $p = e^{-1}he \cdot h^{-1}$ Nun sind verschiedene Fälle möglich:

α) Jeder der Zyklen von h enthält mehr als drei Elemente, so daß etwa $h = (1234\ldots)\ldots$ Setzt man dann $e = (234)$, so wird $p = (124)$, enthält also weniger Elemente als h.

β) h enthält mindestens zwei Zyklen von drei Elementen, so daß etwa $h = (123)(456)\ldots$ Für $e = (125)$ wird dann $p = (15243)$, enthält also wieder weniger Elemente als h.

γ) h enthält mindestens zwei Zyklen von zwei Elementen, so daß etwa $h = (12)(34)\ldots$ Für $e = (123)$ ergibt sich dann $p = (13)(24)$, welches weniger Elemente enthält als h, wenn nicht grade $h = (12)(34)$ ist. In letzterem Falle setze man $e = (125)$ und findet $p = (125)$.

Die Substitutionen von H, welche die geringste Zahl von Elementen enthalten, sind daher alle vom Typus $(a\,b\,c)$, da $(a\,b)$ als ungrade Substitution nicht in H vorkommt.

Nun kann aber jeder Zyklus von drei Elementen in jeden andern solchen Zyklus durch eine grade Substitution transformiert werden, so daß in H alle dreigliedrigen Zyklen vorkommen. Denn (123) kann in $(a\,b\,c)$ durch jede der Substitutionen

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ a & b & c & d & e & \ldots & l \end{pmatrix}, \quad s(de) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ a & b & c & e & d & \ldots & l \end{pmatrix}$$

transformiert werden, wobei man die erste oder zweite Substitution zu wählen hat, je nachdem s grade oder ungrade ist.

Endlich ist jede grade Substitution in ein Produkt dreigliedriger Zyklen zerlegbar. Denn wenn in $e = t_1 t_2 \ldots t_{2k}$, wo die t_i alles Transpositionen sind, t_1 und t_2 gleich sind, so heben sie sich auf; haben sie ein Element gemeinsam, so ist

$$t_1 t_2 = (a\,b)(a\,c) = (a\,b\,c);$$

haben sie schließlich kein Element gemeinsam, so ist

$$t_1 t_2 = (ab) \cdot (cd) = (abc)(cad).$$

Ähnliches gilt natürlich für das übrigbleibende Produkt $t_3 t_4 \ldots t_{2k}$.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Jede invariante Untergruppe H von A ist also mit A identisch. —

Die symmetrische Gruppe von mehr als vier Variabeln hat daher die Kompositionsreihe G, A, E mit den Indizes 2 und $\frac{n!}{2}$. Da letztere Zahl keine Primzahl ist, so ist G nicht auflösbar.

Satz 14: Die allgemeine Gleichung von höherem als viertem Grade ist nicht auflösbar.

Übungen: 1. Die symmetrische Gruppe G von mehr als vier Elementen hat keine andere Kompositionsreihe als G, A, E. Denn wenn G eine invariante Untergruppe $H \neq E$ hat, so zeigt der Beweis von Satz 13, daß entweder $H = A$ oder daß H eine Transposition (ab) enthält. In letzterem Falle aber enthält H jede Transposition und fällt daher mit G zusammen.

2. Wenn die allgemeine Gleichung fünften Grades nicht auflösbar ist, so ist es auch nicht die von noch höherem Grade. — Denn noch nicht einmal die spezielle Gleichung, die man durch Nullsetzen der Koeffizienten von x^j für $j \leqq n - 5$ bekommt, ist ja auflösbar.

3. Wir wollen daher hier noch einen anderen Beweis für Satz 14 geben, indem wie die Einfachheit der alternierenden Gruppe A für $n = 5$ beweisen: Angenommen, $abcde$ sei eine beliebige Permutation von 12345 und entstehe aus letzterer durch die Transformation mit s. — Es gibt nun immer eine grade Substitution, welche (123) in (abc) transformiert. Desgleichen eine solche, welche (12)(34) in $(ab)(cd)$ transformiert, nämlich entweder s selbst oder $(12)s$ [oder $(34)s$], von denen die eine ja immer grade ist. Schließlich kann $t = (12345)$ oder sonst $t^2 = (13524)$ immer durch eine grade Substitution in $k = (abcde)$ übergeführt werden. Für grades s ist dies selbstverständlich; für ungrades s wird t^2 durch das ungrade $l = (3245)$ in t, also durch das grade ls in k transformiert. — Enthält daher eine invariante Untergruppe H von A die Substitution (123) bzw. (12)(34) bzw. (12345), so enthält sie auch (abc) bzw. $(ab)(cd)$ bzw. $(abcde)$. Solcher Substitutionen gibt es aber 20 bzw. 15 bzw. 24, so daß die Ordnung von H gleich $h = 1 + 20x + 15y + 24z$ ist, wo x, y, z nur die Werte 0 oder 1 annehmen können. Zugleich ist h ein eigentlicher Teiler von 60. Enthält nun h den Faktor 5, so muß $x = 0, y = 0, z = 1$, also $h = 25$ sein. Da dies kein Teiler von 60 ist, so muß h ein Teiler von $\frac{60}{5}$ sein, das gibt aber nur die Möglichkeit $h = 1$.

4. Wenn für einen Bereich K die Gruppe einer Gleichung mit den Wurzeln $x_1, \ldots, x_n$ die Erzeugende $s = (x_1 x_2 \ldots x_n)$ besitzt, so ist die Gleichung irreduzibel, und es ist x_2 eine rationale Funktion $r(x_1)$ mit Koeffizienten aus K, desgleichen natürlich $x_3 = r(x_2), \ldots, x_n = r(x_{n-1}), x_1 = r(x_n)$. — Umgekehrt besitzt eine irreduzible Gleichung aus K, deren Wurzeln diesen n Beziehungen genügen, in K eine reguläre zyklische Gruppe.

Denn da die Gruppe transitiv ist, so ist die Gleichung nach Satz 7 irreduzibel. Jede Wurzel, also auch x_1, gehört zu E. Adjungiert man also x_1, so sind alle Wurzeln in $K(x_1)$ enthalten, so daß z. B. $x_2 = r(x_1)$.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

5. Durch eingehendere Behandlung von Übung 3 zeige man, daß jede Substitution der alternierenden Gruppe von fünf Elementen konjugiert zu E, (123), $(12)(34)$, $t = (12345)$ oder t^2 ist.

114. Auflösbare Gleichungen fünften Grades. Die Jacobi-Cayleysche Resolvente sechsten Grades einer Gleichung fünften Grades wurde kürzlich vom Verfasser[1]) auf direkte, elementare Weise aufgestellt. Die Gleichung fünfter Ordnung ist dann und nur dann lösbar, wenn ihre Resolvente eine rationale Wurzel hat. Ebenso wurden auf einfache Weise die kovarianten Resolventen von Perrin und McClintock abgeleitet.

Berwick[2]) berechnete eine Resolvente sechsten Grades, deren Koeffizienten Invarianten der entsprechenden Gleichung fünfter Ordnung sind.

---

1) Bull. Amer. Math. Soc. 31, 1925, pp. 515—523. Betreffs dieser und anderer Resolventen vergleiche man Brioschi, Math. Annalen 13, 1878, pp. 109 bis 160.

2) Proc. London Math. Soc. (2), 14, 1915, pp. 301—307.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

ZWÖLFTES KAPITEL.

KONSTRUKTIONEN MIT ZIRKEL UND LINEAL.

115. Problemstellung. Wir werden beweisen, daß es in der Euklidischen Geometrie unmöglich ist, einen beliebigen Winkel in drei gleiche Teile zu teilen, ebenso ein reguläres 7- oder 9-Eck zu konstruieren. Vergeblich suchten daher die alten Griechen, diese Aufgaben mit Benutzung von Zirkel und Lineal zu lösen. — Vergeblich versuchten ferner nicht nur die alten Griechen von Euklid an, sondern auch alle Mathematiker der Folgezeit, zu den Werten $n = 2^m$, $n = 3$, $n = 5$ einen weiteren wesentlichen Wert von n zu finden, für den das reguläre n-Eck mit Zirkel und Lineal konstruierbar ist, bis schließlich der 19jährige Gauß die Konstruierbarkeit des 17-Ecks erkannte und damit das erste neue Resultat seit über 2000 Jahren fand! Doch geht seine Entdeckung weit über dieses spezielle Ergebnis hinaus, denn es fand nicht nur den einen Wert 17, sondern alle solchen Werte überhaupt! Und weiter stellte er für alle Werte von n die Gleichungsketten auf, von deren Auflösungen die Lösung der Gleichung für die Ecken des n-Ecks abhängt. — Das erste dieser Resultate werden wir in 116. ableiten.

116. Das analytische Kriterium für die Konstruierbarkeit mit Zirkel und Lineal. Unser erster Schritt, um die Lösbarkeit einer vorgelegten Konstruktionsaufgabe zu untersuchen, besteht darin, das Problem analytisch zu formulieren. — Bei dem alten Delischen Problem der Verdoppelung des Würfels nehmen wir als Längeneinheit eine Seite des gegebenen Würfels, dann ergibt sich die Seite x des gesuchten Würfels aus der Gleichung $x^3 = 2$.

Zur Aufgabe der Dreiteilung eines gegebenen Winkels A verwenden wir die Identität

$$\cos A = 4\cos^3\frac{A}{3} - 3\cos\frac{A}{3}. \tag{1}$$

Setzt man hier $x = 2\cos\frac{A}{3}$, so erhält man

$$x^3 - 3x - 2\cos A = 0. \tag{2}$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Ist A gegeben, so können wir (mit Zirkel und Lineal) eine Strecke von der Länge $|\cos A|$ konstruieren. Sie ergibt sich als eine Kathete eines rechtwinkligen Dreiecks mit dem Winkel A und der Hypotenuse 1. Wenn nun die Dreiteilung von A, also die Konstruierbarkeit von $\frac{1}{3}A$ möglich wäre, so könnten wir eine Strecke von der Länge $\left|\cos\frac{A}{3}\right|$, also auch x selbst konstruieren.

So sind wir bei beiden Problemen auf eine kubische Gleichung gestoßen, deren Wurzel geometrisch konstruierbar sein muß, wenn das Problem selbst lösbar ist.

Kriterium 1[1]): Damit eine reelle Wurzel x einer gegebenen Gleichung mit Zirkel und Lineal konstruierbar ist, ist notwendig und hinreichend, daß sich das Aufsuchen der Wurzel auf die Lösung einer endlichen Kette von linearen und quadratischen Gleichungen (mit reellen Wurzeln) zurückführen läßt.

Zunächst ist die Bedingung hinreichend, denn eine lineare Gleichung läßt sich mittels der vier elementaren Rechenoperationen auflösen. Die Operationen $a+b$, $a-b$, $a\cdot b$, $a:b$ sind aber geometrisch mit dem Lineal ausführbar. — Die Lösung einer quadratischen Gleichung führt auf eine lineare und eine rein quadratische Gleichung. Eine Strecke von der Länge $\sqrt{n}$, wo $n>0$, läßt sich aber finden, z. B. nach dem Höhensatz des Euklid als mittlere Proportionale zu 1 und n.

Nehmen wir umgekehrt an, wir könnten die Wurzel x einer Gleichung aus den Koeffizienten der Gleichung, die uns als Strecken gegeben sind, konstruieren. Jede Teilaufgabe mit dem Lineal allein, d. h. das Verbinden von Punkten oder das Zum-Schnitt-Bringen von Geraden, führt auf die Lösung linearer Gleichungen, jede Teilaufgabe mit Lineal und Zirkel, d. h. das Auffinden der Schnittpunkte einer Geraden und eines Kreises, auf die Lösung einer linearen und einer quadratischen Gleichung, endlich jede Teilaufgabe mit dem Zirkel allein, d. h. das Auffinden der Schnittpunkte zweier Kreise, auf die Lösung zweier quadratischer Gleichungen, die sich in diesem Fall auf die Lösung einer linearen und einer quadratischen Gleichung zurückführen läßt. Die ganze Aufgabe besteht also in analytischer Hinsicht in der Lösung einer Kette linearer und quadratischer Gleichungen.

---

1) Descartes, La Géométrie, Leyde 1638, livre premier (Deutsche Ausgabe von Schlesinger, Berlin 1894).

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Kriterium 2: (Satz von Wantzel und Petersen.) Damit — ausgehend vom Bereich K — eine Gleichung sich auf eine Kette linearer und quadratischer Gleichungen zurückführen läßt, ist notwendig (aber nicht hinreichend!), daß die Ordnung ihrer Gruppe für K eine Potenz von 2 ist (vgl. 104., Folg.).

117. Verdopplung des Würfels, Dreiteilung des Winkels. In R ist die Gruppe von $x^3 - 2 = 0$ die symmetrische Gruppe G_6 von der Ordnung 6. Nach Kriterium 2 ist daher die Verdopplung des Würfels mit Lineal und Zirkel unmöglich.

Die Gleichung (2) für die Dreiteilung des Winkels besitzt im allgemeinen in $R(\cos A)$ als Gruppe die symmetrische. Auch die Dreiteilung des Winkels mit Zirkels und Lineal ist daher im allgemeinen unmöglich.[1])

Z. B. ist die Dreiteilung von $A = 120^0$ unmöglich. Denn da $\cos 120^0 = -1$, so wird die zugehörige Gleichung

$$x^3 - 3x + 1 = 0. \tag{3}$$

Diese ist aber nach 83., Übung 3 in R irreduzibel, und, da ihre Diskriminante gleich 81 ist, die alternierende Funktion also den rationalen Wert ± 9 hat, so ist (vgl. Beisp. in 92.) für R ihre Gruppe die alternierende von der Ordnung 3.

Soll also die Dreiteilung eines Winkels möglich sein, so muß die Gruppe seiner zugehörigen Gleichung die Ordnung 2 haben. Das ist aber nur möglich, wenn der Bereich $R(\cos A)$ die Größe $\cos \frac{A}{3}$ schon enthält, d. h. wenn $\cos \frac{A}{3}$ rational ist, etwa gleich $\frac{a}{b}$, wo a und b ganze Zahlen sind. Dann ist aber $\cos A = (4a^3 - 3ab^2) : b^3$. Umgekehrt, wenn $\cos A = (4a^3 - 3ab^2) : b^3$, so ist A mit Zirkel und Lineal in drei Teile teilbar.

Übungen: 1. Es ist unmöglich, einen Winkel in drei gleiche Teile zu teilen, wenn sein Kosinus gleich $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{8}$ oder $p:q$ ist, wo p und q teilerfremde ganze Zahlen sind und wo q keinen kubischen Faktor enthält.

2. Ein reguläres 9-Eck kann nicht mit Lineal und Zirkel konstruiert werden. — Denn sein Winkel 40^0 kann nicht konstruiert werden, da 120^0 nicht in drei gleiche Teile geteilt werden kann. Ein anderer Beweis ergibt sich daraus, daß die zugehörige Gleichung $x^6 + x^3 + 1 = 0$ (vgl. 85.) nach 108. eine reguläre zyklische Gruppe von der Ordnung 6 besitzt.

---

1) Für einen elementaren Beweis ohne Benutzung der Gruppentheorie vgl. man eine Abhandlung des Verfassers im Amer. Math. Monthly 21, 1914, pp. 259—262.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

3. Es ist unmöglich, mit Zirkel und Lineal einen Quader mit der Diagonale 5, der Oberfläche 24 und dem Volumen 1, 2, 3 oder 5 zu konstruieren.

4. Es ist unmöglich, die Höhe eines Kugelsegmentes zu konstruieren, welches den vierten Teil des Inhaltes der Kugel besitzt (Problem des Archimedes). Denn man wird im wesentlichen auf die Gleichung (3) geführt.

118. Reguläre Polygone. Das Problem der Dreiteilung des Winkels kann verallgemeinert werden zu dem der n-Teilung. Spezialisiert man wieder den Winkel zu 2π, so ist diese Konstruktion des Winkels $\frac{2\pi}{n}$ äquivalent der Konstruktion des regulären n-Ecks. Die Koordinaten der Ecken dieses regulären n-Ecks hängen aber von der Kreisteilungsgleichung $x^n = 1$ ab. Eine ihrer Wurzeln ist $x = \cos\frac{2\pi}{n} + i \cdot \sin\frac{2\pi}{n}$. Da $\frac{1}{x} = \cos\frac{2\pi}{n} - i \cdot \sin\frac{2\pi}{n}$, so ist $x + \frac{1}{x} = 2\cos\frac{2\pi}{n}$. Hierdurch sind wir von dem komplexen Wert x auf eine reelle Größe $\cos\frac{2\pi}{n}$ übergegangen. Jetzt ist also Kriterium 1 anwendbar. Nach ihm ist x durch i und reelle Quadratwurzeln ausdrückbar, wenn $\cos\frac{2\pi}{n}$ durch reelle Quadratwurzeln darstellbar ist, und umgekehrt. Ein n-Eck kann daher dann und nur dann mit Zirkel und Lineal konstruiert werden, wenn das Aufsuchen einer Wurzel von $x^n = 1$ sich auf die Lösung einer Kette linearer und quadratischer Gleichungen zurückführen läßt.

Nun läßt sich die Gleichung $x^{ab} = 1$, wo a und b teilerfremd sind, auf die Lösung der beiden Gleichungen $x^a = 1$ und $x^b = 1$ zurückführen. Denn wenn die Wurzeln von $x^a = 1$ mit ξ_i und die b Wurzeln von $x^b = 1$ mit η_k bezeichnet werden, so daß also ${\xi_i}^a = 1$ bzw. ${\eta_k}^b = 1$, so sind alle $a \cdot b$ Produkte $\xi_i \cdot \eta_k$ voneinander verschieden und sind die Wurzeln von $x^{ab} = 1$. Der zugehörige Winkel $\frac{2\pi}{ab}$ wird aus $\frac{2\pi}{a}$ und $\frac{2\pi}{b}$ gefunden, indem man zwei ganze, der Gleichung $ap - bq = 1$ genügende Zahlen p und q bestimmt (was nach 80. möglich ist). Dann ist

$$\frac{2\pi}{ab} = p \cdot \frac{2\pi}{b} - q\frac{2\pi}{a}.$$

Umgekehrt bekommen wir aus dem $a \cdot b$-Eck durch Verbinden der Ecken $1, b+1, 2b+1, \ldots, (a-1)\cdot b + 1$ ein a-Eck.

Ist also $n = p^e q^f \ldots$, wo $p, q, \ldots$ voneinander verschiedene Primzahlen sind, so ist die Konstruktion des regulären n-Ecks voll-

Digitized by Google Original from UNIVERSITY OF MICHIGAN

kommen äquivalent den Konstruktionen der Polygone mit den Seitenzahlen p^s, q^t, ...

Wir können uns daher auf den Fall $n = p^s$, wo p eine ungrade Primzahl ist, beschränken. Die primitiven p^sten Einheitswurzeln genügen dann einer in R irreduziblen Gleichung (85.) vom Grade $e = p^{s-1}(p-1)$, die für R eine reguläre zyklische Gruppe von der Ordnung e besitzt (108.). Ist diese Gleichung durch eine Kette quadratischer Gleichungen lösbar, so muß (nach Kriterium 2) e eine Potenz von 2 sein. Für $s > 1$ ist dies aber unmöglich, da dann e den ungraden Faktor p besitzt. Es muß also $s = 1$, d. h. $e = p - 1$ sein. Ist nun $e = 2^{at}$, wo a ungrade ist, so hat $p = 2^{at} + 1$ den Faktor $2^t + 1$, ist also keine Primzahl. Wenn daher ein reguläres p^s-Eck, wo p eine ungrade Primzahl ist, konstruiert werden kann, so ist $s = 1$ und p von der Form

$$2^{2^k} + 1. \tag{4}$$

Für $k = 0, 1, 2, 3, 4$, erhält man für p die Werte 3, 5, 17, 257, 65537, also lauter Primzahlen. Hingegen sind die Werte von p, die sich aus $k = 5, 6, 7, 8, 9, 11, 12$ ergeben, keine Primzahlen.

Ist umgekehrt p eine Primzahl der Form (4), so ist die Konstruktion des regulären p-Ecks möglich, denn die zugehörige Gleichung besitzt für R eine reguläre zyklische Gruppe von der Ordnung $p - 1 = 2^{2^k}$, deren Indexreihe aus lauter Zweien besteht. Dann reduziert sich aber nach 106. die Gleichung auf eine Kette quadratischer Gleichungen.

Verbindet man dieses Resultat mit obigem und bedenkt noch, daß ein 2^k-Eck sich immer konstruieren läßt, so erhält man den

Satz: Ein reguläres n-Eck kann dann und nur dann mit Zirkel und Lineal konstruiert werden, wenn $n = 2^k \cdot p_1 \cdot p_2 \cdot p_3 \cdots$, wo $p_1, p_2, \ldots$ voneinander verschiedene Primzahlen der Form (4) sind.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

DREIZEHNTES KAPITEL.

POLYEDERGRUPPEN. GLEICHUNGEN FÜNFTEN GRADES.

119. Einleitung. Der erste Teil dieses Kapitels enthält eine Theorie der Invarianten jeder endlichen Gruppe linearer Transformationen von zwei Variablen. Diese Gruppen sind isomorph zu Gruppen von Drehungen, welche die zugehörigen regulären Polyeder in sich selbst überführen. — Im Schlußteil besprechen wir eine Anwendung auf die Resolventen der allgemeinen Gleichung fünften Grades und geben eine Methode zur Lösung dieser Gleichung. Diese Anwendung ist in der Theorie der Modul- und automorphen Funktionen von großer Wichtigkeit.

Die Theorie stammt von Klein, dessen klassisches Werk[1]) indessen durch die aus vielen Teilen der Mathematik entlehnten Begriffe dem Anfänger ziemliche Schwierigkeiten bereitet. Wir werden hier das Wichtigste dieser interessanten Theorie auf einfache Weise entwickeln.

120. Die einer Drehung zugeordnete lineare Transformation. Obgleich Lesern, die mit der Theorie der Funktionen vertraut sind, ein kürzerer Beweis der Formel (7) geläufig ist[2]), wollen wir es doch nicht unterlassen, hier einen ganz elementaren Beweis zu geben.

Wir denken uns eine Einheitskugel mit dem Ursprung eines rechtwinkligen Koordinatensystems als Mittelpunkt. Von ihrem „Nordpol" aus projizieren wir sie stereographisch auf die gegenüberliegende Koordinatenebene, d. h. wir denken uns alle Punkte der Kugel mit dem Nordpol durch Geraden verbunden und diese Geraden mit der erwähnten Ebene zum Schnitt gebracht. Dadurch bekommen wir eine ein-eindeutige Korrespondenz zwischen den Punkten der Kugel und den Punkten einer Ebene, die wir als die komplexe Gaußsche Ebene annehmen wollen. Nur für den Nordpol

1) Vorlesungen über das Ikosaeder, 1884.

2) Burkhardt, Funktionentheorie I, 2, 1903, pp. 49—52.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

selbst hört die Abbildung auf, stetig zu sein. Wir heben diese Unstetigkeit dadurch, daß wir das nach dem Unendlichen hin offene Kontinuum der komplexen Ebene durch Hinzufügung eines einzigen Punktes, nämlich $z = \infty$, zu einem abgeschlossenen Kontinuum ergänzen. Dann entspricht der Nordpol dem Punkte $z = \infty$, und unsere Abbildung ist überall stetig und umkehrbar eindeutig.

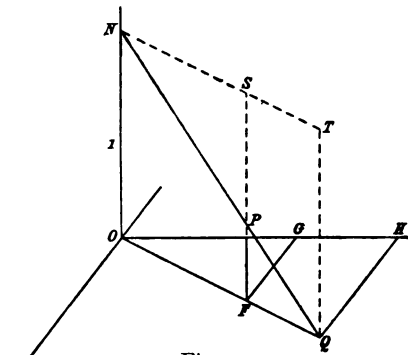

Fig. 1.

Wir wollen nun die Beziehung zwischen dem Kugelpunkt $P = (\xi, \eta, \zeta)$ und dem Punkt $z = x + iy$ der Gaußschen Ebene — d. h. hier der $\xi\eta$-Ebene — aufsuchen. In Fig. 1 ist $N = (0, 0, 1)$, $Q = (x, y, 0)$, $NT \parallel OQ$, $PSF \parallel NO$, FG und HG parallel der η-Achse, $Og = \xi$, $FG = \eta$, $FP = \zeta$, $OH = x$, $QH = y$. Da $\Delta NSP \sim \Delta NTQ$, so ist

$$(1 - \zeta) : 1 = SP : TQ = NS : NT = OF : OQ = \eta : y = \xi : x,$$

also

$$(1) \qquad x = \frac{\xi}{1-\zeta}, \quad y = \frac{\eta}{1-\zeta}, \quad \text{d. h.} \quad z = \frac{\xi + i\eta}{1-\zeta}.$$

Da nun

$$(2) \qquad \xi^2 + \eta^2 + \zeta^2 = 1,$$

so ist wegen

$$1 + x^2 + y^2 = \frac{(1-\zeta)^2 + \xi^2 + \eta^2}{(1-\zeta)^2} = \frac{1 - 2\zeta + 1}{(1-\zeta)^2} = \frac{2}{1-\zeta},$$

$$(3) \quad \xi = 2x : r, \quad \eta = 2y : r, \quad \zeta = 1 - 2 : r, \quad r = 1 + x^2 + y^2.$$

Jetzt sei $E = (\lambda, \mu, \nu)$ ein beliebiger Punkt der Kugel, und man drehe die Kugel im Gegenzeigersinn (wenn man von E nach O blickt) um OE als Achse durch den Winkel α. Dann setze man

$$(4) \quad a = \lambda \cdot \sin\frac{\alpha}{2}, \quad b = \mu \cdot \sin\frac{\alpha}{2}, \quad c = \nu \cdot \sin\frac{\alpha}{2}, \quad d = \cos\frac{\alpha}{2},$$

so daß also

$$(5) \qquad a^2 + b^2 + c^2 + d^2 = 1.$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Durch die Drehung gehe (ξ, η, ζ) in (ξ', η', ζ') über. Unter Benutzung der Formeln (28) von 46. für die Drehung bekommen wir dann, wenn wir a_1, a_2, a_3 durch a, b, c, w_1, w_2, w_3 durch ξ, η, ζ und p_1, p_2, p_3 durch ξ', η', ζ' ersetzen, aus (3) oder der damit äquivalenten Formel

$$\xi = \frac{z + \bar{z}}{1 + z\bar{z}}, \quad \eta = \frac{i(\bar{z} - z)}{1 + z\bar{z}}, \quad \zeta = \frac{z\bar{z} - 1}{1 + z\bar{z}},$$

wo $\bar{z} = x - iy$,

$$\tfrac{1}{2}(1 + z\bar{z})(1 - \zeta') = c^2 + d^2 + z\bar{z}(1 - c^2 - d^2) + ez + \bar{e}\bar{z},$$

wo wir $bd - ac + i(ad + bc) = (b + ia)(d + ic) = e$ gesetzt haben. Ersetzt man $1 - c^2 - d^2$ durch den gleichen Wert $a^2 + b^2$, so bekommt man

$$\tfrac{1}{2}(1 + z\bar{z})(1 - \zeta') = [(b + ia)z + d - ic] \cdot f,$$

wo $f = (b - ia)\bar{z} + (d + ic)$. —

Ähnlich ist

$$\tfrac{1}{2}(1 + z\bar{z})(\xi' + i\eta') = [(d + ic)z - (b - ia)] \cdot f. \; —$$

Ebenso wie (1) ist für $z' = x' + iy'$

$$z' = \frac{\xi' + i\eta'}{1 - \zeta'}, \qquad \text{d. h.} \tag{6}$$

$$z' = \frac{(d + ic)z - (b - ia)}{(b + ia)z + (d - ic)}. \tag{7}$$

Satz 1: Jeder Drehung der Einheitskugel entspricht eine linear-gebrochene Transformation (7) der Gaußschen Ebene.

Um das Produkt $A\,B$ einer durch (7) definierten Transformation A und einer zweiten Transformation $B: z' = f(z)$ zu finden, schreibe man letztere in der Form $z'' = f(z')$ und eliminiere z' aus der letzten Gleichung und aus (7). Die resultierende Transformation $z'' = \varphi(z)$ ist das verlangte $A\,B$.

Übungen: 1. Aus (4) und (7) beweise man, daß die Drehungen in der z-Ebene durch

$$z' = e^{i\alpha} z \tag{8}$$

dargestellt werden. Denn dann ist $\lambda = \mu = 0$, $\nu = 1$.

2. Aus (8) leite man die Transformationsformeln der analytischen Geometrie her

$$\xi' = \xi \cdot \cos\alpha - \eta \cdot \sin\alpha, \quad \eta' = \xi \cdot \sin\alpha + \eta \cdot \cos\alpha.$$

121. Die Tetraedergruppe. In eine Einheitskugel mit dem Mittelpunkt O sei ein Würfel einbeschrieben. Seine Ecken bilden die

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ecken zweier diametral zueinander liegenden Tetraeder, nämlich 1234 und 1′2′3′4′.

Die Verbindungslinien der Mittelpunkte je zweier gegenüberliegenden Kanten von 1234, nämlich AA', BB', CC' stehen aufeinander senkrecht. Wir nehmen sie daher als die ξ-, η-, ζ-Achse mit den positiven Richtungen OA, OB, OC.

Dreht man das Tetraeder um $O1$, $O2$, $O3$ oder $O4$ als Achse, und zwar um den Winkel 0^0, 120^0 oder 240^0, so wird es in sich selbst übergeführt; desgleichen bei einer Umwendung (d. h. einer Drehung um 180^0) um AA', BB' oder CC'. Das sind (abgesehen von der Nulldrehung) acht Drehungen von der Ordnung drei und drei von der Ordnung zwei. Sie liefern offenbar alle Drehungen, welche das Tetraeder 1234 in sich selbst überführen, und bilden daher eine Gruppe, die sog. Tetraedergruppe R_{12}. Denn es gibt genau drei Drehungen, welche die Ecke 1 nicht verändern, während ihre Produkte mit einer beliebigen der Drehungen (um $O4$), welche 1 in 2 überführen, alle solchen Rotationen ergeben; Ähnliches gilt, wenn wir 3 oder 4 an Stelle von 2 setzen. Die Gesamtzahl der Drehungen ist daher 3×4.

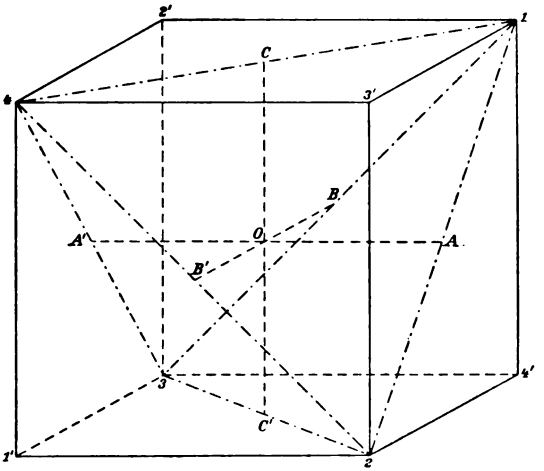

Fig. 2.

Gehen wir jetzt näher ein auf die Drehung S um die Achse $O1$ durch den Winkel 120^0 (im Gegenzeigersinn, wenn man von 1 nach O blickt) und auf die Umwendung U um die Achse CC'. Da 1 und 4 durch U vertauscht werden, so bleibt 4 durch USU und US^2U ungeändert. Letztere sind daher Drehungen um die Achse $O4$, welche 1 nach 3 bzw. 2 schaffen. Nach der letzten Bemerkung im vorigen Abschnitt bekomme ich daher alle Drehungen von R_{12}, wenn ich E, S und S^2 mit US^2U, USU und U — welche ja 1 in 2 bzw. 3 bzw. 4 überführen — multipliziere.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Satz 2: Die Tetraedergruppe R_{12} hat die Erzeugenden S und U.

Wir wollen sofort die linearen Transformationen von z aufstellen, welche nach 120. den Drehungen S und U entsprechen. Im Falle U haben wir in (8) $\alpha = \pi$ zu setzen und bekommen $z' = -z$. — Sodann bildet die Achse $O1$ der Drehung S mit den positiven Koordinatenachsen gleiche Winkel, so daß die Koordinaten von Punkt 1 gleich $\lambda = \mu = \nu = \frac{1}{3}\sqrt{3}$ sind. Wegen $\alpha = 120^0$, $\cos 60^0 = \frac{1}{2}$, $\sin 60^0 = \frac{1}{2}\sqrt{3}$ folgt aus (4) $a = b = c = d = \frac{1}{2}$. Dann bekommt man für (7)

$$z' = \frac{z+i}{z-i}. \tag{9}$$

Satz 3: Die Gruppe G_{12} der linearen Tetraedertransformationen besitzt die Erzeugenden (9) und $z' = -z$.

Übungen: 1. Die Gruppe R_{12} ist einstufig isomorph mit der alternierenden Gruppe von vier Elementen.

2. Die 12 Transformationen von G_{12} sind

$$z' = \pm z,\ \pm z^{-1},\ \pm i\cdot\frac{z+1}{z-1},\ \pm i\cdot\frac{z-1}{z+1},\ \pm\frac{z+i}{z-i},\ \pm\frac{z-i}{z+i}. \tag{10}$$

Anleitung: $S^2 = S^{-1}$ wird durch die dritte Funktion von (10) mit dem oberen Vorzeichen geliefert, während $L = S^{-1}US$ durch $z' = z^{-1}$ dargestellt wird. Letztere kann man entweder aus dem Produkt $S^{-1}US$ berechnen oder so, daß man davon ausgeht, daß L, da es A ungeändert läßt, eine Umwendung von AA' ist. Für $\lambda = 1$, $\mu = \nu = 0$, $\alpha = \pi$ bekommt man aus (4) $a = 1$, $b = c = d = 0$, also wird (7) zu $z' = i : (iz)$.

3. Bedeutet U (oder $z' = -z$) die Umwendung von CC' und L (oder $z' = z^{-1}$) diejenige um AA', so ist ihr Produkt $M = UL$ die Umwendung um das CC' und AA' gemeinsame Lot BB'. Man zeige nun, daß E, U, L, M eine kommutative Gruppe bilden.

Die Transformation (7) nimmt, wenn $z = z_1 : z_2$, $z' = z_1' : z_2'$ gesetzt wird, die homogene Form

$$\begin{aligned} z_1' &= (d + ic)\, z_1 - (b - ia)\, z_2 \\ z_2' &= (b + ia)\, z_1 + (d - ic)\, z_2 \end{aligned} \tag{11}$$

an. Jeder unimodularen Transformation (7) ist also eine unimodulare lineare homogene Transformation (11) zugeordnet; zugleich aber auch diejenige Transformation, die durch Änderung der Vorzeichen von a, b, c, d entsteht, und die daher das Produkt von (11) und $z_1' = -z_1$, $z_2' = -z_2$ ist.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Insbesondere entsprechen $z' = -z = iz:(-i)$ und (9) den Transformationen

$$z_1' = iz_1, \quad z_2' = -iz_2, \tag{12}$$

$$\begin{aligned} z_1' &= \tfrac{1}{2}(1+i)z_1 - \tfrac{1}{2}(1-i)z_2 \\ z_2' &= \tfrac{1}{2}(1+i)z_1 + \tfrac{1}{2}(1-i)z_2. \end{aligned} \tag{13}$$

Satz 4: Die Gruppe H_{24} der linearen homogenen Tetraeder-Transformationen wird durch die unimodularen Transformationen (12) und (13) erzeugt.

122. Die Invarianten der Tetraedergruppe H_{24}. Die Ecken des Tetraeders 1234 haben die Koordinaten

$$\xi = \pm\tfrac{1}{3}\sqrt{3}, \quad \eta = \pm\tfrac{1}{3}\sqrt{\tfrac{1}{3}}, \quad \zeta = \pm\tfrac{1}{3}\sqrt{3}, \tag{14}$$

wo jedesmal eine ungrade Zahl von Vorzeichen positiv ist. Die zugehörigen Werte von z sind nach (6) gleich $\pm a$ und $\pm b$, wo

$$a = \frac{1+i}{-1+\sqrt{3}}, \quad b = \frac{1-i}{1+\sqrt{3}}.$$

Wir suchen das Produkt Φ der Faktoren $z_1 \pm az_2$, $z_1 \pm bz_2$. Unter Berücksichtigung, daß $a^2 = i(2+\sqrt{3})$ und $b^2 = -i(2-\sqrt{3})$ das Produkt 1 und die Summe $2i\sqrt{3}$ haben, bekommen wir

$$\Phi = z_1^4 - 2i\sqrt{3}z_1^2z_2^2 + z_2^4. \tag{15}$$

Da die 12 Drehungen, welche das Tetraeder in sich selbst überführen — die sog. automorphen Drehungen des Tetraeders —, nur die 4 Ecken vertauschen, so werden durch jede der 24 homogenen Tetraedertransformationen die obigen vier linearen Funktionen bis auf konstante Faktoren lediglich permutiert und das Produkt Φ ist daher eine relative Invariante von H_{24}. Der multiplizierende Faktor ist für (12) bzw. (13) gleich 1 bzw.

$$\left[\frac{1}{2}(1+i)\right]^4 \cdot (1-2i\sqrt{3}+1) = \frac{1}{2}(-1+i\sqrt{3}) = e^{\frac{2\pi i}{3}}.$$

Φ^3 bleibt also gegenüber (12) und (13) vollkommen ungeändert, also nach Satz 4 auch gegenüber allen Transformationen von H_{24}, d. h. Φ^3 ist eine absolute Invariante der Gruppe H_{24}.

Die Ecken des diametral gelegenen Tetraeders $1'2'3'4'$ haben ebenfalls die Koordinaten (14), wo aber jetzt eine ungrade Zahl von Vorzeichen negativ ist. Die entsprechenden Werte von z sind

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$\pm \bar{a}$, $\pm \bar{b}$. Die Gruppe H_{24} hat daher auch die absoluten Invarianten $\Phi\Psi$ und Ψ^3, wo

$$\Psi = z_1^4 + 2i\sqrt{3}\, z_1^2 z_2^2 + z_2^4. \quad (16)$$

Jede Drehung, die das Tetraeder 1234 in sich selbst überführt, vertauscht nur dessen 6 Kanten, also auch deren Mittelpunkte und ferner die Punkte, in denen die Koordinatenachsen die Einheitskugel treffen; die entsprechenden Werte von z sind $0, \infty, \pm 1, \pm i$. Das Produkt

$$t = z_1 z_2 (z_1^4 - z_2^4), \quad (17)$$

welches für diese Werte von $z = z_1 : z_2$ verschwindet, ist daher gleichfalls eine absolute Invariante der Gruppe H_{24}, da es sich gegenüber deren Erzeugenden (12) und (13) invariant verhält. —

Ein Kugelpunkt heiße nun ein spezieller Punkt in bezug auf die Tetraedergruppe R_{12}, wenn er bei diesen 12 Drehungen weniger als 12 verschiedene Lagen annimmt. Mit anderen Worten: ein Punkt ist dann und nur dann speziell, wenn er durch mindestens eine dieser Drehungen — von E abgesehen — ungeändert bleibt; er liegt dann auf der Drehungsachse. Umgekehrt sind die Durchstoßungspunkte der zu R_{12} gehörigen Drehungsachsen lauter spezielle Punkte, so daß man auf diese Weise alle solchen Punkte bekommt.

Die Achsen AA', BB', CC' der Drehungen zweiter Ordnung sind die Koordinatenachsen. Sie treffen die Kugel in den sechs speziellen Punkten, für welche die Invariante t verschwindet.

Die acht Drehungen dritter Ordnung von R_{12} haben als Achsen die durch die Tetraederecken gehenden Durchmesser. Diese Ecken sind aber die vier speziellen Punkte, für welche die Invariante Φ verschwindet. Die übrigen Durchstoßungspunkte dieser Durchmesser mit der Kugel sind die Ecken des Diametraltetraeders und sind daher die vier speziellen Punkte, für welche Ψ verschwindet. Es gibt daher im Ganzen 14 spezielle Punkte.

Nun sei ein beliebiges homogenes Polynom in z_1, z_2 gegeben, welches eine (relative) Invariante von H_{24} ist und für einen speziellen Punkt verschwindet. Es enthält dann natürlich t, Φ oder Ψ als Faktor. Verschwindet es für mehrere spezielle Punkte, so enthält es mehrere dieser Faktoren, nach deren Entfernung schließlich ein Quotient Q übrigbleibt, der zwar invariant ist, aber für keinen speziellen Punkt mehr verschwindet, also auch t, Φ oder Ψ nicht mehr als Faktor enthält. Enthält er als Faktoren Polynome in t, Φ und Ψ, so muß jedes dieser Polynome homogen und relativ

Digitized by Google Original from UNIVERSITY OF MICHIGAN

invariant sein. Da aber t schon absolut invariant ist, so sind es auch die Verbindungen, in denen Φ und Ψ vorkommen. Das ist aber nur möglich, wenn in diesen Polynomen Φ und Ψ nur in Potenzen von Φ^3 und Ψ^3 auftreten; dann darf aber gleichzeitig wegen der Homogeneität t nur in Potenzen von t^2 vorkommen. Die einfachste solche Funktion, welche in Q als Faktor enthalten sein könnte, hätte demnach — wenn irgend zwei der Funktionen t^2, Φ^3, Ψ^3 mit f und g bezeichnet werden — die Form $f - c \cdot g$, wo c ein Zahlenfaktor ist. Ob sie wirklich in Q enthalten sein kann, wollen wir jetzt untersuchen. Besitzt $Q(z, 1)$ die Wurzel z', so verschwindet $Q(z_1, z_2)$, da es homogen in z_1, z_2 ist, für $z_1 = z_1', z_2 = z_2'$, wenn $z_1' : z_2' = z'$. Soll nun $f - cg$ ein Faktor von Q sein, so muß es für gewisse Wurzeln von Q, so etwa für z_1', z_2', verschwinden. Durch diese Bedingung ist c eindeutig bestimmt, da z' kein spezieller Punkt, also $g(z_1', z_2') \neq 0$ ist. Da also $f - cg$ eine Wurzel mit Q gemeinsam hat, so hat es, da es invariant unter H_{24} ist, alle Wurzeln mit Q gemeinsam, ist also einer seiner Faktoren. Der Quotient $Q : (f - cg)$ ist entweder eine Konstante oder wieder eine Funktion von der Art wie Q. Fährt man in dieser Weise fort, so kommt man zu

Satz 5: Jedes in H_{24} invariante, homogene Polynom in z_1, z_2 ist ein Produkt von t, Φ, Ψ und von Funktionen der Form $f - cg$, wo die c Konstanten $\neq 0$ sind und f und g irgend zwei der absoluten Invarianten t^2, Φ^3, Ψ^3 vom Grade 12 bedeuten.

Daher ist jede Invariante vom Grade 12, welche für keinen der 14 speziellen Punkte verschwindet, eine absolute Invariante und kann auf eine der Formen $a(t^2 - c\Phi^3)$, $b(t^2 - d\Psi^3)$, wo a, b, c, d von Null verschiedene Konstanten sind, gebracht werden. Daher genügen auch t^2, Φ^3, Ψ^3 einer linearen Gleichung, die sich durch Berechnung der Glieder z_1^{12} und $z_1^{10} z_2^2$ zu

$$12i\sqrt{3}\,t^2 + \Phi^3 - \Psi^3 \equiv 0 \quad \text{ergibt.} \tag{18}$$

Übungen: 1. Sind z und Z die stereographischen Projektionen zweier diametral entgegengesetzter Punkte der Einheitskugel, so ist $\bar{z}Z = -1$. Mittels dieser Beziehung leite man (16) aus (15) her, indem man z in $\bar{\Phi}(z_1, z_2)$ durch $-z^{-1}$ ersetzt.

2. Die Hessesche Form von Φ ist $-48i\sqrt{3}\,\Psi$, die Jacobische Form von Φ und Ψ gleich $32i\sqrt{3}t$. Die Invarianten I und J der biquadratischen Form Φ sind gleich Null bzw. $\frac{4}{9}i\sqrt{3}$. Man sieht, daß (18) nichts anderes ist als die Syzygie (22) aus 12.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

123. Die Oktaedergruppe. In Fig. 2 ist der aus zwei Pyramiden (mit den Spitzen C und C' und dem Quadrat $ABA'B'$ als gemeinsamer Grundfläche) bestehende Körper ein reguläres Oktaeder. Dieses geht in sich selbst über durch die Drehungen der Gruppe R_{12} sowie durch die 12 Drehungen, welche die Ecken von 1234 in die von 1′2′3′4′ übergehen lassen, d. h. durch die 6 Schwenkungen (d. h. Drehungen durch $\pm 90^0$) um die Achsen AA', BB', CC' und die 6 Umwendungen um die 6 Durchmesser, welche je zwei Kanten des Oktaeders halbieren.

Nun kann bei einer automorphen Drehung des Oktaeders jede Ecke höchstens 6 verschiedene Lagen einnehmen, und man erkennt leicht, daß es Produkte obiger Drehungen gibt, die jede Ecke, z. B. A, in jede andere überführen; da es andererseits nur vier Drehungen gibt, die A ungeändert lassen, nämlich die um OA, so ist die Zahl der automorphen Drehungen des Oktaeders höchstens $6 \cdot 4$, also, da wir schon 24 gefunden haben, genau $6 \cdot 4$. Wir bekommen so eine Gruppe R_{24}. Ihre Erzeugenden sind U und S aus 121. und die — wenn man von C nach O blickt, im Gegenzeigersinn ausgeführte — Schwenkung D um die ζ-Achse. Nach (8) wird D durch $z' = iz$ dargestellt; eine der beiden zugehörigen homogenen Transformationen ist daher

$$z_1' = \sqrt{\tfrac{1}{2}}\,(1+i)\,z_1, \quad z_2' = \sqrt{\tfrac{1}{2}}\,(1-i)\,z_2. \tag{19}$$

Satz 6: Alle automorphen Drehungen eines regulären Oktaeders bilden eine Gruppe R_{24}, die eine Obergruppe der Tetraedergruppe R_{12} ist. Die zugehörige Gruppe H_{48} der linearen homogenen Oktaedertransformationen besitzt die Erzeugenden (12) und (13) der TetraederGruppe H_{24} und die Erzeugende (19).

124. Invarianten der Oktaedergruppe H_{48}. Nehmen wir dasjenige Oktaeder, dessen Ecken die Durchstoßungspunkte der drei Koordinatenachsen mit der Einheitskugel sind.

Die Funktion (17) ist, da sie nur für die Ecken des Oktaeders verschwindet, eine Invariante von H_{48}, und zwar eine relative Invariante, da sie nur bei den Transformationen von H_{24} ungeändert bleibt, durch (19) hingegen in ihren negativen Wert übergeht. t^2 ist infolgedessen eine absolute Invariante von H_{48}.

Die Hessesche Form von t ist $-25\,W$, wo

$$W = z_1^{\,8} + 14 z_1^{\,4} z_2^{\,4} + z_2^{\,8} = \Phi\Psi; \tag{20}$$

die Jacobische Form von t und W ist (abgesehen von einem Zahlenfaktor)

$$\chi = z_1^{\,12} - 33 z_1^{\,8} z_2^{\,4} - 33 z_1^{\,4} z_2^{\,8} + z_2^{\,12}. \tag{21}$$

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Da diese beiden Formen Invarianten vom Gewichte 1 bzw. 2 sind (3., 5.) und da t bei allen Transformationen von H_{48} in $\pm t$ übergeht, so ist W eine absolute Invariante von H_{48}, χ hingegen eine relative, da es in $\pm \chi$ übergeführt wird. —

Ein Punkt der Einheitskugel heiße wiederum speziell, wenn er bei wenigstens einer (von E verschiedenen) Drehung von H_{24} ungeändert bleibt, also auf einer Drehungsachse liegt. Zu den 14 speziellen Punkten der Tetraedergruppe R_{12}, welche die Nullstellen von t und $W = \Phi\Psi$ sind, kommen hier nach 123. noch die Punkte hinzu, welche die Zentralprojektionen der Mittelpunkte der 12 Oktaederkanten sind, so daß wir im Ganzen 26 spezielle Punkte haben. Die zugehörige Funktion, welche also für jene letzteren 12 Punkte verschwindet, muß gleich χ sein. Denn χ muß als Invariante für 12 spezielle Punkte verschwinden; diese können aber nicht z. T. mit den früheren zusammenfallen, da sonst χ ein Produkt der Invarianten t und $\Phi\Psi$, also gleich t^2 sein müßte, was aber unmöglich ist, da t^2 absolut invariant ist (vgl. unten Übung 3). — Durch eine ähnliche Diskussion wie in 122. erhalten wir

Satz 7: Jede Form in z_1, z_2, welche bez. der Gruppe H_{48} der linearen Oktaedertransformationen invariant ist, ist ein Produkt von t, W, χ und Ausdrücken der Form $f - cg$, wo c eine Konstante ist und f und g irgend zwei der absoluten Invarianten t^4, W^3, χ^2 vom Grade 24 sind. Letztere genügen der Identität

$$108t^4 - W^3 + \chi^2 \equiv 0. \tag{22}$$

Übungen: 1. Was wird aus Φ und Ψ durch Anwendung der Transformation (19)? Bilde daraus einen neuen Beweis für die Invarianz von $\Phi\Psi$ unter H_{48}.

2. R_{24} ist einstufig isomorph zu der symmetrischen Gruppe von vier Elementen. Denn zu jeder Drehung von R_{24} gehört eine Vertauschung der Würfeldiagonalen $11'$, $22'$, $33'$, $44'$.

3. Der Durchmesser, der die Kante, auf der die Punkte (0, 0, 1) und (1, 0, 0) liegen, halbiert, trifft die Einheitskugel im Punkte $(\frac{1}{2}\sqrt{2}, 0, \frac{1}{2}\sqrt{2})$, für den $z = 1 + \sqrt{2}$. Setzt man nun $z_1 = 1 + \sqrt{2}$, $z_2 = 1$, so wird $\chi = 0$. Die Invariante χ verschwindet also in den Zentralprojektionen der Mittelpunkte aller 12 Kanten.

4. Die Invarianten jeder endlichen Gruppe G linearer Transformationen besitzen ein vollständiges System. Denn nach dem Hilbertschen Satz (17.) ist jede Invariante I von G in der Form $I \equiv E_1 I_1 + \cdots + E_m I_m$ ausdrückbar, wo die I_k Invarianten sind. Man wende die Transformationen von G an und addiere. — Warum gilt dieser Beweis auch für relative Invarianten?

Digitized by Google Original from UNIVERSITY OF MICHIGAN

125. Die Ikosedergruppe. Wir gehen aus von einem regulären Ikosaeder I, welches einer Einheitskugel mit dem Mittelpunkt O einbeschrieben ist. Es besitzt 20 dreieckige Seitenflächen, 12 Ecken und 30 Kanten. — V sei eine der Ecken. Dann bleibt I bei der — wenn man von V nach O blickt — im Gegenzeigersinn um OV durch den Winkel $\frac{2\pi}{5}$ ausgeführten Drehung S ungeändert. Bezeichnet man die in V zusammenstoßenden Dreiecke mit A_0VA_1, $A_1VA_2, \ldots, A_4VA_0$, so bringt S die Ecke A_0 nach A_1, A_1 nach $A_2, \ldots, A_4$ nach A_0. Für den Augenblick bezeichnen wir einmal die Umwendung um die Achse, welche O mit dem Mittelpunkt einer Kante AB verbindet, mit $[AB]$; I bleibt durch $[AB]$ natürlich ungeändert. Dann schreiben wir noch T anstatt $[A_0V]$. Da nun S den Mittelpunkt von A_0V in den von A_1V überführt, so läßt $S^{-1}TS$ letzteren Punkt ungeändert und ist daher gleich $[A_1V]$. Ähnlich ist $S^{-k}TS^k = [A_kV]$. Wir nennen diese 5 Umwendungen $[A_kV]$ und die 5 Potenzen von S „die 10 mit V verbundenen Drehungen". Sie haben die Erzeugenden S und T. Durch $[A_kV]$ werden sie in die 10 mit A_k verbundenen Drehungen übergeführt, da $[A_kV]$ die Ecke V mit A_k vertauscht. S und T sind daher die Erzeugenden aller mit $A_0, A_1, A_2, A_3, A_4, V$ verbundenen Drehungen. Es läßt sich vermuten, daß sie die Erzeugenden aller Drehungen überhaupt sind. In der Tat, ist A_0B eine der beiden von A_0 ausgehenden, aber von A_0A_4, A_0V, A_0A_1 verschiedenen Kanten, so kann ich — ähnlich wie eben aus den mit V verbundenen Drehungen die mit A_0 verbundenen — jetzt aus den mit A_0 verbundenen Drehungen die mit B verbundenen erhalten. Eine von diesen schafft dann A_0 nach V'. — Ich kann somit durch passend gewählte Produkte von S und T die Ecke V in alle 11 anderen Ecken überführen. Und da die 5 Potenzen von S die einzigen Drehungen sind, die V ungeändert lassen, so gibt es genau 5×12 automorphe Drehungen von I.

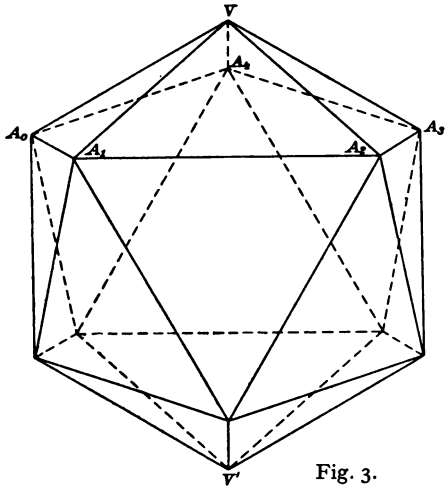

Fig. 3.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Satz 8: S und T sind die Erzeugenden der Ikosaedergruppe R_{60}, d. h. der Gruppe der automorphen Drehungen von I.

Übungen: 1. Da T die Ecke V mit A_0 sowie A_1 mit A_4 vertauscht, so ist das Produkt $ST = (VA_0A_4) \ldots$ eine Drehung von der Ordnung 3, deren Achse den Mittelpunkt von VA_0A_4 mit O verbindet.

2. Die 60 Drehungen von R_{60} setzen sich folgendermaßen zusammen: 1. aus E, 2. den 6×4 Drehungen fünfter Ordnung um die 6 durch die Ecken gehenden Durchmesser, 3. den 15 Umwendungen um die durch die Mittelpunkte zweier Kanten gehenden Durchmesser und 4. (Übg. 1) den 2×10 Drehungen dritter Ordnung um die durch die Mittelpunkte zweier Flächen gehenden Durchmesser.

126. Die lineare homogene Ikosaedergruppe H_{120}. OV nehme man als die positive ζ-Achse eines Koordinatensystems, die ξ-Achse lege man so, daß die Achse von T im zweiten und vierten Quadranten der $\xi\zeta$-Ebene liegt. Dann wird nach (8) S durch $z' = \varepsilon z$ oder durch eine der beiden zugehörigen homogenen Formen, etwa

$$z_1' = \varepsilon^3 z_1, \quad z_2' = \varepsilon^2 z_2, \quad \text{wo} \quad \varepsilon = e^{\frac{2\pi i}{5}}, \tag{23}$$

dargestellt. Der Ecke A_0 entspricht eine reelle negative Zahl n. Da werden A_i durch S in A_{i+1} übergeht, so werden A_1, A_2, A_3, A_4 durch $\varepsilon n, \varepsilon^2 n, \varepsilon^3 n, \varepsilon^4 n$ dargestellt. — Ferner vertauscht T die Ecken A_0 und V, die durch n bzw. ∞ dargestellt werden, sowie die diametral entgegengesetzten Punkte $m = -n^{-1}$ und O, so daß

$$T: \qquad z' = \frac{nz + 1}{z - n}.$$

Ferner vertauscht T die Ecke A_1 mit A_4, führt also $z = \varepsilon n$ in $z' = \varepsilon^4 n$ über, so daß $n^2(1 - \varepsilon - \varepsilon^4) = 1$ oder $n^2(\varepsilon + \varepsilon^4)^2 = 1$, d. h., da $\varepsilon + \varepsilon^4 > 0$ und $n < 0$, $n(\varepsilon + \varepsilon^4) = -1$. Transformiert man m und n durch die Potenzen von S $(z' = \varepsilon z)$, so sieht man, daß die 12 Ecken des Ikosaeders durch

$$z = 0, \quad \infty, \quad \varepsilon^k m, \quad \varepsilon^k n \qquad (k = 0, 1, 2, 3, 4;\ m = \varepsilon + \varepsilon^4;\ n = \varepsilon^2 + \varepsilon^3) \tag{24}$$

dargestellt werden.

Erweitert man T mit $\varepsilon^3 - \varepsilon^2$, so erhält man

$$T: \qquad z' = \frac{(\varepsilon - \varepsilon^4)z + (\varepsilon^3 - \varepsilon^2)}{(\varepsilon^3 - \varepsilon^2)z - (\varepsilon - \varepsilon^4)}$$

mit der Determinante 5. In homogener Form hat daher T die Gestalt

$$\begin{aligned} z_1'\sqrt{5} &= (\varepsilon - \varepsilon^4)z_1 + (\varepsilon^3 - \varepsilon^2)z_2, \\ z_2'\sqrt{5} &= (\varepsilon^3 - \varepsilon^2)z_1 - (\varepsilon - \varepsilon^4)z_2. \end{aligned} \tag{25}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Zur Kontrolle berechne man das Quadrat hiervon und erhält $z_1' = -z_1$, $z_2' = -z_2$, wie es sein muß.

Satz 9: Die Ikosaedergruppe H_{120} hat die Erzeugenden (23) und (25).

127. Invarianten der Ikosaedergruppe. Die Form, welche die 12 Werte (24) von $z = z_1 : z_2$ zu Nullstellen hat, ist

$$f = z_1 z_2 (z_1^5 - m^5 z_2^5)(z_1^5 - n^5 z_2^5).$$

Um dies auszumultiplizieren, suchen wir die Summe s_5 der fünften Potenzen der Wurzeln von $x^2 + x - 1 = 0$, nämlich $m^5 + n^5$. Durch Multiplikation mit x^{r-2}, Einsetzen der Wurzeln und Summieren erhält man die Rekursionsformel

$$s_r + s_{r-1} - s_{r-2} = 0,$$

also für s_5 den Wert

$$s_5 = -s_4 + s_3 = 2s_3 - s_2 = -3s_2 + 2s_1 = 5s_1 - 6 = -11.$$

Dann wird f, da $mn = -1$, zu

$$f = z_1 z_2 (z_1^{10} + 11 z_1^5 z_2^5 - z_2^{10}). \tag{26}$$

Schließlich ist die Hessesche Form von f gleich $121H$, die Jacobische Form von f und H gleich $20J$, wo

$$H = -z_1^{20} - z_2^{20} + 228 (z_1^{15} z_2^5 - z_1^5 z_2^{15}) - 494 z_1^{10} z_2^{10} \tag{27}$$

$$J = z_1^{30} + z_2^{30} + 522 (z_1^{25} z_2^5 - z_1^5 z_2^{25}) - 10005 (z_1^{20} z_2^{10} + z_1^{10} z_2^{20}). \tag{28}$$

—

Ein spezieller Punkt wird wie früher definiert. Die Aufzählung der Drehungen in Übung 3 des vorigen Paragraphen zeigt dann, daß jeder solche Punkt zu einer der folgenden Gruppierungen gehören muß: 1. der Gesamtheit der 12 Ecken (für die f verschwindet), 2. den 20 Zentralprojektionen der Mittelpunkte der Dreiecksflächen, 3. den 30 Zentralprojektionen der Mittelpunkte der Kanten. Wir haben daher im ganzen 62 spezielle Punkte. — Nun sind H und J Kovarianten des Ikosaeders, verschwinden also für gewisse spezielle Punkte. Da aber ein Aggregat von zwei oder mehr der obigen Komplexe (wobei auch ein Komplex mehrmals vorkommen darf) niemals ein System von 20 oder 30 Punkten geben kann, so sind die Nullstellen von H und J nichts anderes als die beiden letzten oben angeführten Komplexe. f, H, J sind daher die einzigen (relativen) Invarianten der Gruppe H_{120}.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Nun ist f eine absolute Invariante von H_{120}, da es weder durch (23) geändert wird noch, wie man durch Ausrechnung beweist, durch (25). Dasselbe ist aber auch für H und J der Fall, da alle Transformationen unimodular sind. -- Ebenso wie in 122. erhalten wir den

Satz 10: Jede ganze rationale Invariante der Ikosaedergruppe H_{120} ist absolut invariant und ist ein Polynom in f, H, J, zwischen denen die Identität

$$J^2 \equiv 1728 f^5 - H^3 \quad \text{besteht.} \tag{29}$$

128. Das Formenproblem des Tetraeders und Oktaeders. Nach 122. ist jede ganzrationale absolute Invariante der homogenen Tetraedergruppe H_{24} ein Polynom in den absoluten Invarianten t, $W = \Phi\Psi$ und Φ^3, zwischen denen die Identität

$$\Phi^3[12i\sqrt{3}\,t^2 + \Phi^3] - W^3 \equiv 0 \tag{30}$$

besteht. Wir schreiben nun t, W, Φ^3 beliebige, jedoch mit (30) verträgliche Werte vor und suchen diejenigen Wertsysteme von z_1, z_2, für welche t, W und Φ^3 jene vorgeschriebenen Werte annehmen. Man nennt dies das „Formenproblem von H_{24}". Aus jeder Lösung für z_1, z_2 erhalten wir durch Anwendung der Transformationen von H_{24} offenbar 23 neue Lösungen. Wir werden jedoch beweisen, daß es bei jedem solchen vorgeschriebenen Wertsystem auch tatsächlich nur 24 Lösungen gibt: Man führe dazu die Funktionen

$$Y_1 = \Phi^6 : W^3 = \Phi^3 : \Psi^3 \equiv Y_1\left(\frac{z_1}{z_2}\right), \quad X(z_1, z_2) = W : t \tag{31}$$

ein. Die Werte Y_1 und X dieser absolutinvarianten Funktionen sind natürlich ebenfalls vorgeschrieben. Da Y_1 eine Funktion von $\frac{z_1}{z_2}$ ist, so können wir aus der zugehörigen Gleichung

$$(z^4 - 2i\sqrt{3}z^2 + 1)^3 - Y_1(z^4 + 2i\sqrt{3}z^2 + 1)^3 = 0 \tag{32}$$

das Verhältnis $z = \frac{z_1}{z_2}$ ausrechnen. Bedenken wir nun, daß W bzw. t den Grad 8 bzw. 6 besitzt, X als homogen vom Grade 2 ist, so sehen wir, daß $X(z_1, z_2) = z_2^2 \cdot X(z, 1)$. Hieraus läßt sich z_2 berechnen und schließlich aus $z = \frac{z_1}{z_2}$ auch z_1. Nun liefert die Gleichung (32) 12 Werte für z, und die Gleichungen

$$z_2^2 = X(z_1, z_2) : X(z, 1), \quad z_1 = z \cdot z_2 \tag{33}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

liefern für jeden solchen Wert wiederum zwei Lösungen, so daß wir im ganzen 24 Lösungen des Problems erhalten. Das Formenproblem für H_{24} reduziert sich also auf die Lösung der Gleichung (32) und auf das Ziehen von Quadratwurzeln. Erstere wollen wir noch etwas genauer untersuchen.

Die Gleichung (32) ist in der Gruppe G_{12} der lineargebrochenen Tetraedertransformationen von z invariant. Vier unter diesen, nämlich (vgl. Übung 3, 121.) $z' = \pm z$, $z' = \pm z^{-1}$, lassen die Funktion

$$Y_2 = (z^2 - 1)^2 : 4z^2 \tag{34}$$

invariant. Bezeichnet man mit ω die dritte Einheitswurzel $\frac{1}{2}(-1 + i\sqrt{3})$, so ist

$$\begin{aligned} Y_2 - \omega &= (z^4 - 2i\sqrt{3}z^2 + 1) : 4z^2 \\ Y_2 - \omega^2 &= (z^4 + 2i\sqrt{3}z^2 + 1) : 4z^2, \qquad \text{demnach} \end{aligned}$$

$$\left(\frac{Y_2 - \omega}{Y_2 - \omega^2}\right)^3 = Y_1. \tag{35}$$

Die Gleichung (32) wird daher zurückgeführt auf eine Kette von Gleichungen niedrigerer Grade, nämlich auf die reinkubische Gleichung (35) für Y_2, die in z^2 quadratische Gleichung (34) und eine reinquadratische Gleichung für z. Das Formenproblem des Tetraeders ist daher durch Radikale lösbar. —

Beim Formenproblem der Oktaedergruppe H_{48} sind für die absoluten Invarianten $W, t^2, t\chi$ willkürliche, jedoch mit (22) oder

$$t^2(108t^4 - W^3) + (t\chi)^2 \equiv 0$$

verträgliche Werte vorgeschrieben. Gesucht werden wieder die dazugehörigen 48 Wertsysteme von z_1, z_2. Setzt man

$$Y = \frac{W^3}{t^4}, \quad X(z_1, z_2) = \frac{Wt}{\chi}, \tag{36}$$

so ist X wiederum[1]) vom Grade 2 in z_1, z_2, und wir haben daher wieder Gleichung (33). Setzen wir ferner wieder $Y_1 = \Phi^3 : \Psi^3$, so folgt aus (30) und $W = \Phi\Psi$, daß

$$(-3) \cdot 144 Y_1 : (Y_1 - 1)^2 = Y. \tag{37}$$

Nun sind die Werte von Y und X durch die gegebenen Werte von $W, t^2, t\chi$ mitbestimmt. Die erste Gleichung (36) ist vom Grade 24

1) Natürlich ist dieses X ein anderes als das von (31) und (33)!

Digitized by Google Original from UNIVERSITY OF MICHIGAN

in der Unbekannten $z = \frac{z_1}{z_2}$; sie läßt sich jedoch reduzieren auf die in Y_1 quadratische Gleichung (37) und auf die früheren Gleichungen, die aus Y_1 den Wert für z ergaben. Aus z lassen sich schließlich durch (33) z_1 und z_2 berechnen.

Satz 11: Die Formenprobleme des Tetraeders und Oktaeders sind durch Radikale lösbar.

129. Das Formenproblem des Ikosaeders. Für beliebig vorgeschriebene, jedoch mit (29) verträgliche Werte der absoluten Invarianten f, H, J suchen wir die 120 zugehörigen Wertsysteme von z_1, z_2. Durch die bisherigen Untersuchungen wird uns nahegelegt, wieder eine Funktion von $z = \frac{z_1}{z_2}$ zu suchen; als solche bietet sich $\frac{f^5}{J^2}$. Wir brauchen demnach nur die Gleichungen

$$Z = \frac{f^5}{J^2}, \quad X(z_1, z_2) = \frac{fH}{J} \tag{38}$$

zu lösen. Da X quadratisch ist, so haben wir wieder Gleichung (33). Das Formenproblem reduziert sich also im wesentlichen auf die Lösung der Gleichung $f^5 + Z \cdot J^2 = 0$, welche nach Division mit z_2^{60} in

$$z^5(z^{10} + 11z^5 - 1)^5 - Z[z^{30} + 1 + 522(z^{25} - z^5) - 10005(z^{20} + z^{10})]^2 = 0 \tag{39}$$

übergeht. Diese Gleichung 60. Grades, die nur den einen Parameter Z enthält, heißt die Ikosaedergleichung. Im Gegensatz zu den Formenproblemen des Tetraeders und Oktaeders ist sie durch Radikale nicht lösbar. Unser erster Schritt führt die Gleichung (39) auf eine wichtige Gleichung fünften Grades zurück.

In (26) stellten wir die Funktion f auf, welche in den zwölf Ecken des Ikosaeders I verschwindet. Offenbar bleibt nun f durch die Transformation

$$z_1' = -z_2, \quad z_2' = z_1 \quad \text{oder} \quad z' = -z^{-1} \tag{40}$$

ungeändert. Also geht I durch die entsprechende Drehung F in sich selbst über, so daß (40) zu H_{120} gehört. In 121., Übung 3 sahen wir, daß F die Umwendung um die η-Achse und TF die Umwendung um die gemeinsame Senkrechte der Achse von F und T ist (T war nach 125., 126. die Umwendung um die Senkrechte zu A_0V).

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Um die Fixpunkte (d. h. die Punkte, die sich bei der Transformation nicht verändern) von (40) zu erhalten, hat man nur $z' = z$ zu setzen und bekommt daraus $z^2 + 1 = 0$. Ähnlich erhält man die Fixpunkte von T, indem man nämlich in der inhomogenen Schreibweise von (25) wieder $z' = z$ setzt. Ebenso für TF. Schließlich ersetze man in den entstehenden drei Gleichungen z durch $\frac{z_1}{z_2}$. Dann werden die Ruhepunkte von F, T, TF durch die Nullstellen von

$$A_0 = z_1^2 + z_2^2, \quad B_0 = z_1^2 - 2(\varepsilon^2 + \varepsilon^3) z_1 z_2 - z_2^2,$$
$$C_0 = z_1^2 - 2(\varepsilon + \varepsilon^4) z_1 z_2 - z_2^2$$

geliefert. Die Nullstellen von

$$(41) \quad t_0 = A_0 B_0 C_0 = z_1^6 + 2 z_1^5 z_2 - 5 z_1^4 z_2^2 - 5 z_1^2 z_2^4 - 2 z_1 z_2^5 + z_2^6$$

entsprechen demnach den Ecken eines regulären Oktaeders. t_0 ist daher (ähnlich wie t in 124.) die Fundamentalinvariante der Oktaedergruppe (bezogen allerdings auf andere Achsen als die von 124.). Wir wollen nun untersuchen, welchen Einfluß die Substitutionen der Ikosaedergruppe auf t_0, A_0, B_0, C_0 haben, vor allem also die Erzeugenden S und T.

Nach (23) entspricht S^k der homogenen Substitution

$$(42) \qquad S^k: \quad z_1' = \varepsilon^{3k} z_1, \quad z_2' = \varepsilon^{2k} z_2.$$

Durch sie gehen A_0, B_0, C_0 über in

$$A_k = \varepsilon^k z_1^2 + \varepsilon^{4k} z_2^2, \quad B_k = \varepsilon^k z_1^2 - 2(\varepsilon^2 + \varepsilon^3) z_1 z_2 - \varepsilon^{4k} z_2^2,$$
$$C_k = \varepsilon^k z_1^2 - 2(\varepsilon + \varepsilon^4) z_1 z_2 - \varepsilon^{4k} z_2^2.$$

Man setze $t_k = A_k B_k C_k$. Bemerkt man, daß für das durch (25) definierte T die Beziehung gilt

$$z_1' z_2' = \tfrac{1}{5} l (z_1^2 + z_1 z_2 - z_2^2), \quad \text{wo} \quad l = (\varepsilon^3 - \varepsilon^2)(\varepsilon - \varepsilon^4) = \sqrt{5},$$

so ergibt sich leicht, daß A_1 durch T in $m B_2$ übergeht, wo

$$m = \tfrac{1}{5}(2\varepsilon - \varepsilon^2 + \varepsilon^3 - 2\varepsilon^4),$$

C_1 in $(\varepsilon^2 - \varepsilon^3) A_2$ und $C_1 - B_1 = -2 l z_1 z_2$

in $\quad -2(z_1^2 + z_1 z_2 - z_2^2) = (\varepsilon^2 - \varepsilon^3) A_2 - (\varepsilon^2 + \varepsilon^3) C_2.$

B_1 wird demnach in $(\varepsilon^2 + \varepsilon^3) C_2$ transformiert. Da ferner $m(\varepsilon^2 - \varepsilon^3)(\varepsilon^2 + \varepsilon^3) = 1$, so geht $t_1 = A_1 B_1 C_1$ in t_2 über. Daraus folgt, daß t_4 durch T in t_3 transformiert wird, da A_{-k}, B_{-k}, C_{-k}

Digitized by Google Original from UNIVERSITY OF MICHIGAN

aus A_k, B_k, C_k hervorgehen, wenn man — was lediglich die Vorzeichen der Koeffizienten von T umkehrt, eine quadratische Funktion von z_1, z_2 also nicht beeinflußt — ε durch ε^{-1} ersetzt.

Nun vertauscht T die Endpunkte der Achsen von F und TF, läßt hingegen die von T selbst natürlich ungeändert. Infolgedessen nehmen die zugeordneten Funktionen A_0 und C_0 ihre entgegengesetzten Werte an, während B_0 ungeändert bleibt. Da schließlich T involutorisch, d. h. von der Ordnung 2 ist, so haben wir

$$T = (t_0)(t_1 t_2)(t_3 t_4), \quad S = (t_0 t_1 t_2 t_3 t_4). \tag{43}$$

Da also T und S beides grade Substitutionen von fünf Buchstaben sind und da sie eine Gruppe von 60 Elementen erzeugen, so ist diese Gruppe nichts anderes als die alternierende Gruppe von fünf Buchstaben.

Satz 12: Die Ikosaedergruppe der 60 Drehungen oder der 60 lineargebrochenen Transformationen ist einstufig isomorph zu der alternierenden Gruppe von fünf Buchstaben.

Dasselbe läßt sich auch geometrisch zeigen: Die 15 Durchmesser, die je zwei Kanten des Ikoseders halbieren, zerfallen in fünf Tripel, deren jedes (ähnlich wie die Achsen von F, T, TF) aus drei aufeinander senkrecht stehenden Durchmessern besteht. Die Drehungen von R_{60} führen jedes Tripel in jedes andere über. Es gibt daher $\frac{60}{5} = 12$ Drehungen von R_{60}, welches ein gegebenes Tripel ungeändert lassen; sie bilden eine Untergruppe von R_{24} (deren Elemente vierter Ordnung ja nicht in R_{60} vorkommen), d. h. eine Tetraedergruppe R_{12}. — Es ist nicht schwer, aus (43) die 12 Substitutionen herauszugreifen, welche t_0 ungeändert lassen und daher der Untergruppe R_{12} von R_{60} entsprechen. Z. B. erzeugen $STS^3 = (0)(2)(143)$, T und $F = S^2TS^3TS^2T = (0)(14)(23)$ die homogene Form H_{24} von R_{12}.

Da $t_0, \ldots, t_4$ nach (43) durch jede Transformation der Ikosaedergruppe H_{120} lediglich permutiert werden und daher ihre elementarsymmetrischen Funktionen ungeändert bleiben, so sind $t_0, \ldots, t_4$ die Wurzeln einer Gleichung fünften Grades

$$t^5 + c_1 t^4 + c_2 t^3 + c_3 t^2 + c_4 t + c_5 = 0.$$

Die c_k sind dabei nach (41) vom Grade $6k$ in z_1, z_2. Der größte Wert von $6k$ ist 30. Da dies kleiner als 60 ist und da die c_k Invarianten von H_{120} sind, so sind sie nach 127. Produkte von f, H, J. Deren Gradzahlen sind aber 12 bzw. 20 bzw. 30, also kann keines der erwähnten Produkte den Grad 6 oder 18 besitzen, infolgedessen ist $c_1 = c_3 = 0$ und ähnlich $c_2 = af$, $c_4 = bf^2$, $c_5 = cJ$, wo a, b, c Konstanten sind. Die Koeffizienten in unserer obigen

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Gleichung sind demnach bekannt, wenn a, b, c bekannt sind. Um letztere zu berechnen, stellen wir die Newtonschen Identitäten für die Potenzsummen der Wurzeln unserer Gleichung auf; da $c_1 = c_3 = 0$, so vereinfachen sie sich zu $s_2 + 2c_2 = 0$, $s_4 + c_2 s_2 + 4c_4 = 0$, so daß wir zur Bestimmung von a, b, c die folgenden Gleichungen haben:

$$s_2 + 2af = 0, \quad s_4 + (4b - 2a^2) f^2 = 0, \tag{44}$$
$$cT + t_0 t_1 t_2 t_3 t_4 = 0.$$

Da nun die Transformation S^k aus (42) t_0 durch t_k ersetzt, so ist nach (41)

$$t_k = \varepsilon^{3k} z_1^6 + 2\varepsilon^{2k} z_1^5 z_2 - 5\varepsilon^k z_1^4 z_2^2 + \cdots, \tag{45}$$

und

$$t_k^2 = \varepsilon^k z_1^{12} + 4 z_1^{11} z_2 - 6\varepsilon^{4k} z_1^{10} z_2^2 + \cdots,$$
$$t_k^4 = \varepsilon^{2k} z_1^{24} + 8\varepsilon^k z_1^{23} z_2 + 4 z_1^{22} z_2^2 + \cdots$$

Demnach sind die Koeffizienten von $z_1^{11} z_2$ bzw. $z_1^{22} z_2^2$ bzw. z_1^{30} in den Funktionen (44) gleich

$$20 + 2a = 0, \quad 20 + 4b - 2a^2 = 0, \quad c + 1 = 0,$$

so daß sich für a, b, c die Werte -10, 45, -1 ergeben. Damit haben wir

Satz 13: Die Oktaederformen $t_0, \ldots, t_4$ sind die Wurzeln der Gleichung

$$t^5 - 10ft^3 + 45f^2 t - J = 0. \tag{46}$$

Diese Gleichung wurde zuerst von Brioschi[1]) aufgestellt, welcher zeigte, daß sich jede Gleichung fünften Grades auf diese Form bringen läßt. —

Wir wollen noch in (46) an Stelle von t die Größe $w = \frac{tf^2}{J}$ einführen, da sie eine Funktion von $z = \frac{z_1}{z_2}$ ist. Setzen wir dann nach (38) $Z = \frac{f^5}{J^2}$, so erhalten wir

$$w^5 - 10Zw^3 + 45Z^2 w - Z^2 = 0. \tag{47}$$

130. Die Hauptresolvente fünften Grades der Ikosaedergleichung. In 99. hatten wir den Begriff der Resolvente kennengelernt und hatten gesehen, daß sich durch Adjunktion einer Wurzel einer

1) Annali di Mat. 1, 1858, pp. 256—259, pp. 326—328.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Resolvente der Grad der Gleichung erniedrigt. Wir werden hier eine solche Resolvente für unsere Ikosaedergleichung aufstellen. Dazu ist es gut, wenn wir vorher einige Bemerkungen über gewisse Normalformen von Gleichungen vorausschicken.

Es war lange bekannt, daß sich eine Gleichung

$$g(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

durch die einfache Transformation $y = x + \frac{a_1}{n}$ auf eine Gleichung zurückführen läßt, in der der Koeffizient von y^{n-1} fehlt. Tschirnhausen zeigte nun[1]), daß sich „allgemeinere Transformationen angeben lassen, durch die sich beliebig viele Glieder einer Gleichung wegheben". Diese Transformationen haben die Form

$$y = \frac{h(x)}{q(x)},$$

wo h und q Polynome in x sind und wo q keine Nullstelle mit $g(x)$ gemeinsam haben darf. Hier interessiert uns insbesondere diejenige Transformation, durch welche das zweit- und dritthöchste Glied zum Verschwinden gebracht werden. Eine so transformierte Gleichung nennen wir eine Hauptgleichung; (46) war z. B. eine solche. Wir dürfen annehmen, daß schon $a_1 = 0$. Nach den Newtonschen Identitäten ist dann $s_1 = 0$, $s_2 = -2a_2$. Man führe jetzt die Transformation $y = x^2 + ax + b$ aus und bezeichne mit y_k den Wert $y(x_k)$, wo x_k eine Wurzel der Ausgangsgleichung ist. Da in der Gleichung für y der Koeffizient von y^{n-1} und y^{n-2} verschwinden soll, so muß $\sum y_k$ und $\sum y_k^2$ verschwinden. Nun ist $\sum y_k = s_2 + nb$ dann gleich Null, wenn $b = -\frac{s_2}{n}$. Da ferner

$$y^2 = x^4 + 2ax^3 + (a^2 + 2b)x^2 + 2abx + b^2,$$

so liefert $\sum y_k^2 = s_4 + 2as_3 + (a^2 + 2b)s_2 + nb^2 = 0$

für a zwei Werte. Mit einem von ihnen berechnet man die Potenzsummen $\sum y_k^3$, $\sum y_k^4$, ... und daraus nach den Newtonschen Identitäten die Koeffizienten der Gleichung mit den Wurzeln $y_1, \ldots, y_n$. — Wir haben damit gezeigt, daß die Reduktion einer Gleichung auf eine Hauptgleichung das Lösen einer quadratischen Gleichung erfordert. —

---

1) Acta Eruditorum 2, 1683, pp. 204—207.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Kehren wir jetzt zu unserem Problem zurück. Wir hatten gesehen, daß die t_i einer Gleichung fünften Grades genügen. Dasselbe läßt sich aber auch noch von allgemeineren Größen beweisen:

Die Hessesche Kovariante von t_k ist gleich $400\,W_k$, wo

$$(48)\quad W_k = -\varepsilon^{4k}z_1^{\,8} + \varepsilon^{3k}z_1^{\,7}z_2 - 7\varepsilon^{2k}z_1^{\,6}z_2^{\,2} - 7\varepsilon^{k}z_1^{\,5}z_2^{\,3} + 7\varepsilon^{4k}z_1^{\,3}z_2^{\,5} - 7\varepsilon^{3k}z_1^{\,2}z_2^{\,6} - \varepsilon^{2k}z_1z_2^{\,7} - \varepsilon^{k}z_2^{\,8}.$$

Da nun die Erzeugenden S und T der Ikosaedergruppe H_{120} unimodular sind und $t_0, \ldots, t_4$ nach (43) permutieren, so permutieren sie auch ihre Hesseschen Kovarianten (und also auch $W_0, \ldots, W_4$) auf die gleiche Weise. Für beliebige r und s bleibt daher $\sum t_k^{\,r} W_k^{\,s}$ durch S und T ungeändert, ist infolgedessen eine Invariante von H_{120} und daher ein Polynom in f, H, J. Da diese aber die Gradzahlen 12 bzw. 20 bzw. 30 haben, so kann keine ihrer Kombinationen den Grad 8, 14, 16, 22 oder 28 haben. Demnach ist

$$\sum W = 0, \quad \sum tW = 0, \quad \sum W^2 = 0, \quad \sum tW^2 = 0, \quad \sum t^2W^2 = 0.$$

Setzt man daher

$$(49)\quad X_k = \sigma W_k + \tau t_k W_k \qquad (k = 0, 1, 2, 3, 4),$$

so ist auch $\sum X = 0$, $\sum X^2 = 0$. Da also die zweit- und dritthöchsten Koeffizienten verschwinden, so genügen die X einer Hauptgleichung, deren allgemeine Form $X^5 + \alpha X^2 + \beta X + \gamma = 0$ oder

$$(50)\quad X^5 + 5aX^2 + 5bX + c = 0$$

ist. Es handelt sich jetzt noch darum, die a, b, c zu bestimmen. Nach den Newtonschen Identiäten ist $\sum X^3 = -15\,a$, $\sum X^4 = -20\,b$. Die folgenden Identitäten bekommen wir durch Vergleich der Gradzahlen der beiden Seiten und durch Berechnen je eines einzigen Gliedes:

$$\begin{aligned}
&\sum W^3 = -5\cdot 24 f^2, && \sum tW^3 = -5J,\\
&\sum t^2W^3 = -5\cdot 72 f^3, && \sum t^3W^3 = -15 fJ,\\
&\sum W^4 = 20 fH, && \sum tW^4 = 0,\\
&\sum t^2W^4 = -60 f^2H, && \sum t^3W^4 = -5HJ,\\
&\sum t^4W^4 = -540 f^3H. &&
\end{aligned}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Daraus ergibt sich

$$a = 8\sigma^3 f^2 + \sigma^2\tau J + 72\sigma\tau^2 f^3 + \tau^3 f J$$
$$b = -\sigma^4 f H + 18\sigma^2\tau^2 f^2 H + \sigma\tau^3 H J + 27\tau^4 f^3 H.$$

Um c zu berechnen, beachte man, daß nach (46)

$$x^5 - 10 f x^3 + 45 f^2 x - J \equiv \prod (x - t_k)$$

für alle x. Für $x = -\frac{\sigma}{\tau}$ erhält man hieraus

$$\prod(\sigma + \tau t_k) = \sigma^5 - 10\sigma^3\tau^2 f + 45\sigma\tau^4 f^2 + \tau^5 J.$$

Nun ist aber, wie man auf ähnliche Weise wie oben feststellt, $\prod W_k = -H^2$. D. h.

$$c = -\prod X_k = H^2(\sigma^5 - 10\sigma^3\tau^2 f + 45\sigma\tau^4 f^2 + \tau^5 J).$$

Damit haben wir die Koeffizienten a, b, c gefunden. Um jedoch eine Resolvente der Ikosaedergleichung (39) zu erhalten, müssen wir zu einer Gleichung fünften Grades übergehen, welche f, H, J nur in den Verbindungen

$$Z = \frac{f^5}{J^2}, \quad V = \frac{H^3}{f^5}$$

enthält. Zwischen Z und V besteht nach (29) die Identität

$$Z^{-1} + V = 1728. \tag{51}$$

Setzt man dann noch

$$\sigma = \lambda \frac{f}{H}, \quad \tau = \mu \frac{f^3}{HJ}, \tag{52}$$

so wird

$$\begin{aligned} V \cdot a &= 8\lambda^3 + \lambda^2\mu + (72\lambda\mu^2 + \mu^3)Z, \\ V \cdot b &= -\lambda^4 + 18\lambda^2\mu^2 Z + \lambda\mu^3 Z + 27\mu^4 Z^2, \\ V \cdot c &= \lambda^5 - 10\lambda^3\mu^2 Z + 45\lambda\mu^4 Z^2 + \mu^5 Z^2. \end{aligned} \tag{53}$$

Setzt man diese Werte von a, b, c in (50) ein, so erhält man eine Gleichung, von der wir später (Satz 17) beweisen werden, daß sie eine Resolvente der Ikosaedergleichung, die sog. Hauptresolvente, ist.

131. Die Hauptresolvente ist eine allgemeine Hauptgleichung fünften Grades. Wir werden beweisen, daß die so erhaltene Resolvente keine spezielle Form besitzt, sondern daß jede Hauptgleichung fünften Grades als eine solche Resolvente aufgefaßt werden kann. Dazu haben wir zu zeigen, daß wir für beliebige a, b, c Werte für λ, μ, Z, V angeben können, welche die Gleichungen (51) und (53) erfüllen.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Addieren wir zunächst zu der dritten Gleichung (53), die mit λ multiplizierte zweite, so erhalten wir die mit $\mu^2 Z$ multiplizierte erste, d. h. es ist

$$\lambda b + c = \mu^2 Z a. \tag{54}$$

Multiplizieren wir die dritte mit λ, die zweite mit $\mu^2 Z$ und subtrahieren, so ergibt sich

$$V(\lambda c - \mu^2 Z b) = (\lambda^2 - 3\mu^2) Z^3. \tag{55}$$

Aus den beiden ersten Gleichungen (53) folgt

$$V(\lambda a + 8b)/\mu = \lambda^3 + 216\lambda^2\mu Z + 9\lambda\mu^2 Z + 216\mu^3 Z^2.$$

Dividieren wir das Quadrat dieser Gleichung durch Z, subtrahieren das Ergebnis von dem mit 27 multiplizierten Quadrat der ersten Gleichung (53) und vereinfachen mit Zuhilfenahme von (51), so erhalten wir $V(\lambda^2 - 3\mu^2 Z)^3$. Unter Berücksichtigung von (55) folgt hieraus

$$27a^2 - \frac{(\lambda a + 8b)^2}{\mu^2 Z} = \lambda c - \mu^2 Z b.$$

Eliminiert man hier $\mu^2 Z$ vermittels (54), so haben wir

$$\lambda^2(a^4 + abc - b^3) - \lambda(11a^3 b - ac^2 + 2b^2 c) + (64a^2 b^2 - 27a^3 c - bc^2) = 0. \tag{56}$$

Aus dieser quadratischen Gleichung läßt sich λ ausrechnen. Dann bestimmt man hintereinander $\mu^2 Z$ aus (54), V aus (55) und Z aus (51). Mit Hilfe des sich daraus ergebenden Wertes von μ^2 und der ersten Gleichung (53) ist schließlich μ rational ausdrückbar.

In dem Ausdruck für die Wurzel λ kommt die Diskriminante Δ von (56) vor. Bezeichnet man das Quadrat der Produkte der Wurzeldifferenzen der durch (50) definierten Gleichung $g(X) = 0$ mit P, so ergibt sich für P — da es bekanntlich die Resultante von $g(X)$ und ihrer Ableitung ist — der Wert $P = 5^5 D$, wo

$$D = 108a^5 c - 135a^4 b^2 + 90a^2 bc^2 - 320ab^3 c + 256b^5 + c^4.$$

Man findet nun durch Ausrechnung, daß $\Delta = a^2 D$. [In der Invariantentheorie heißt D, nicht P, die Diskriminante von (50)].

Demnach lassen sich λ, μ, Z, V für beliebige a, b, c aus den Gleichungen (53) und (51) ausrechnen und als rationale Funktionen von a, b, c, $\sqrt{D}$ ausdrücken.

Satz 14: Jede Hauptform einer Gleichung fünften Grades läßt sich als Hauptresolvente der Ikosaedergleichung auffassen. Die einzige Irrationalität, die man nötig hat, ist die Quadratwurzel aus der Diskriminante der Hauptgleichung.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

132. Die allgemeine Gleichung fünften Grades. Wir sahen in 130., daß sich mit Hilfe einer Quadratwurzel eine Transformation angeben läßt, durch welche die allgemeine Gleichung fünften Grades in eine Hauptform übergeht. Ferner bewiesen wir soeben, daß letztere mit der Hauptresolvente von 130., in der λ, μ, Z, V Konstanten sind, identifiziert werden kann; ihre Wurzeln

$$X_k = \frac{\lambda f W_k}{H} + \frac{\mu f^3 t_k W_k}{HJ} \qquad (k = 0, \ldots, 4) \tag{57}$$

sind vom Grade Null in z_1, z_2 und daher Polynome in $z = \frac{z_1}{z_2}$. Demnach läßt sich die allgemeine Gleichung fünften Grades mit Hilfe von zwei Quadratwurzeln und einer Wurzel z der Ikosaedergleichung (39) auflösen. Letztere wiederum ist mittels elliptischer Modulfunktionen[1]) lösbar. Sehen wir also mit Klein eine Wurzel $z = \varphi(Z)$ der Ikosaedergleichung als bekannt an, so lassen sich auch die Wurzeln der allgemeinen Gleichung fünften Grades berechnen.

133. Transformation der Resolvente (47) in die Hauptresolvente. Für das in 121.—124. verwendete Koordinatensystem entsprechen die Nullstellen der Hesseschen Kovariante der Oktaederform t denjenigen Kugelpunkten, welche auf Achsen von Drehungen dritter Ordnung liegen. Da dasselbe auch für das Koordinatensystem von 126., 129., 130. zutrifft, so verschwindet die Hessesche Kovariante W der neuen Form t für solche Werte von z, welche den Mittelpunkten der Dreiecksflächen des Ikosaeders entsprechen. Demnach ist W ein Faktor von H. Ein anderer Faktor ist $t^2 - 3f$; denn wenn wir in (46) das absolute Glied J auf die andere Seite schaffen, quadrieren und t^2 durch $3f$ ersetzen, so erhalten wir

$$3f(24f^2)^2 \equiv 1728 f^5 = J^2,$$

also nach (29) $H = 0$; H verschwindet daher durch die Substitution $t^2 = 3f$, d. h. $t^2 - 3f$ ist ein Faktor von H. Durch Vergleich der Koeffizienten je eines einzelnen Gliedes erhält man schließlich

$$H \equiv W(t^2 - 3f). \tag{58}$$

Mit diesem Wert gehen wir in (57) ein (lassen die k dabei der Einfachheit halber weg), setzen $t = \frac{wJ}{f^2}$ und $Z = \frac{f^5}{J^2}$ und erhalten

$$X = \frac{\lambda + \mu w}{Z^{-1} w^2 - 3}. \tag{59}$$

1) Klein, Math. Annalen 14, 1879, p. 157f. Bianchi, ibid. 17, 1881, pp. 254—257. Klein, Ikosaeder, 1884, pp. 130—136; Theorie der elliptischen Modulfunktionen I, 1890, p. 125.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Transformiere ich also in (47) die Variable w durch die Transformation (59), welche sich ja auf die Form (49) bringen läßt, so erhalte ich die Hauptresolvente von 130.

Satz 15: Durch die Tschirnhausensche Transformation (59) *geht die Resolvente* (47) *in die Hauptresolvente von 130. über.*

Da (47) eine Gleichung fünften Grades ist, die sich gut zur Auflösung durch elliptische Funktionen eignet, so können wir die Hauptresolvente und daher auch jede andere Gleichung fünften Grades mit diesen Mitteln lösen.

Übung: Man gebe für Satz 15 einen direkten Beweis. Aus (47), seinem Produkt mit w, der in w quadratischen, zu (59) gehörigen Gleichung und deren Produkte mit w, w^2, w^3, w^4 eliminiere man nach der Sylvesterschen Eliminationsmethode die Unbekannte w. Man zeige, daß die entstehende Determinante mit (50) übereinstimmt, wenn a, b, c durch (53) und (51) gegeben sind.

134. Die Galoissche Gruppe der Ikosaedergleichung. F_{60} bedeute die Transformationsgruppe

$$z' = L_i(z) \qquad (i = 1, \ldots, 60)$$

der lineargebrochenen Formen der homogenen Transformationen der Ikosaedergruppe. Da letztere die Erzeugenden (23) und (25) haben, so ist ε die einzige in den $L_i(z)$ vorkommende Irrationalität. $I(z)$ bedeute die linke Seite der Ikosaedergleichung (39). Ihre Koeffizienten gehören zu dem Körper $K = R(Z, \varepsilon)$ und sind in der Gruppe F_{60} invariant. Ist demnach z_1 eine Wurzel von $I(z) = 0$, so erhalten wir alle ihre anderen Wurzeln durch die Transformation $z_i = L_i(z_1)$ für $i = 1, \ldots, 60$. Da also jeder Faktor von $I(z)$, dessen Koeffizienten in K liegen, alle 60 Wurzeln zu Nullstellen hat, so ist $I(z)$ in K irreduzibel.

Wegen der Gruppeneigenschaft von F_{60} ist $L_i[L_j(z)] \equiv L_k(z)$. Daher wird durch die Substitution $z_1 \rightarrow z_j$ eine Substitution S_j der 60 Wurzeln $z_i = L_i(z_1)$ induziert.

Wir werden beweisen, daß der Komplex dieser 60 Substitutionen S_j die charakteristischen Eigenschaften A und B der Galoisschen Gruppe von $I(z) = 0$ für K besitzt. Zu dem Zwecke sei $f(z_1, \ldots, z_{60})$ irgendeine rationale Funktion der z_i mit Koeffizienten aus K. Sie möge, wenn man jedes z_i durch $L_i(z_1)$ ersetzt, in $\varphi(z_1)$ mit Koeffizienten aus K übergehen.

Bleibt nun zunächst f durch alle Substitutionen S_j dem Werte nach ungeändert, so sind $\varphi(z_1), \ldots, \varphi(z_{60})$ alle gleich. Ihre Summe

Digitized by Google Original from UNIVERSITY OF MICHIGAN

$60f$ ist eine symmetrische Funktion der Wurzeln von $I(z) = 0$ mit Koeffizienten aus K. D. h. f ist eine Größe aus K.

Umgekehrt sei f gleich einer Größe q aus K. Dann ist $\varphi(z) = q$ eine Gleichung mit Koeffizienten aus K, welche eine Wurzel z_1 mit der in K irreduziblen Gleichung $I(z) = 0$ gemeinsam hat und daher (nach 82.) für alle ihre Wurzeln z_i verschwindet. Mit anderen Worten, die $\varphi(z_i)$ sind alle gleich, so daß f durch die Substitutionen S_j seinem Werte nach ungeändert bleibt.

Satz 16: Die Galoissche Gruppe G der Ikosaedergleichung (39) ist im Bereich $R(Z, \varepsilon)$ einstufig isomorph mit der Gruppe F_{60} der lineargebrochenen Ikosaedertransformationen.

Nach Satz 12 ist daher G auch einstufig isomorph mit der alternierenden Gruppe von fünf Elementen. Demnach ist (113.) die Ikosaedergleichung nicht durch Radikale lösbar. —

Satz 17: Die Lösung der Ikosaedergleichung ist äquivalent zu der Lösung der Resolvente (47) vom fünften Grade, und umgekehrt.

Denn aus einer Wurzel z von (39) können wir sofort die rationalen Funktionen $w_k = \frac{t_k f^2}{J}$ von z berechnen und haben damit die Wurzeln von (47). — Haben wir umgekehrt die Wurzeln w_k von (47) gefunden, so können wir z und daher alle Wurzeln von (39) als rationale Funktionen von w_k, Z, ε ausdrücken. Denn nach Satz 12 ist die Identität die einzige Substitution von F_{60}, welche jedes t_k und daher auch jedes w_k ungeändert läßt, so daß die Identität auch die einzige Substitution von G ist, welche jedes w_k automorph transformiert. Adjungiert man demnach alle w_k zu K, so reduziert sich G auf die Identität, so daß jede Wurzel von (39) in dem erweiterten Bereich enthalten ist.

Übungen: 1. Die Lösung der Hauptresolvente der Ikosaedergleichung ist äquivalent zu der Lösung der letzteren Gleichung. Daher sind die Wurzeln der Hauptresolvente rationale Funktionen von Z und den Wurzeln der Resolvente (47), und umgekehrt. Auf Grund dieser Tatsache hätten wir schon die Existenz einer Tschirnhausen-Transformation voraussagen können, welche (47) in die Hauptresolvente überführt (vgl. 133.).

2. Die Ikosaedergleichung ist ihre eigene Galoissche Resolvente.

3. Für einen Körper, der Z_1 und $\sqrt{-3}$ enthält, ist die Tetraedergleichung (32) ihre eigene Galoissche Resolvente, und ihre Galoissche Gruppe ist einstufig isomorph zu G_{12} und daher auch zu der alternierenden Gruppe von vier Elementen. Demnach ist (32) durch Radikale lösbar.

135. Weitere Ergebnisse. Die Lösung der allgemeinen Gleichung fünften Grades läßt sich zurückführen auf das Formenproblem

Digitized by Google Original from UNIVERSITY OF MICHIGAN

einer Gruppe von 60 linearen Transformationen von drei Variablen.[1]) — Die allgemeine Gleichung sechsten Grades konnte auf das Formenproblem der Valentiner-Gruppe von 360 ternären linearen Transformationen, die zu der alternierenden Gruppe von sechs Elementen einstufig isomorph ist, zurückgeführt werden.[2]) — Die allgemeine Gleichung siebenten Grades reduziert sich auf das Formenproblem einer linearen Gruppe von der Ordnung $\frac{1}{2}7!$ von vier Variablen.[3])

Die symmetrische Gruppe von n Elementen kann dargestellt werden als lineare homogene Gruppe der Variablen $x_1, \ldots, x_n$, die der Beziehung $\sum x_i = 0$ unterworfen sind (vgl. 138.). Jedoch für $n > 7$ ist weder die symmetrische noch die alternierende Gruppe von n Elementen einstufig isomorph zu einer linearen Gruppe von $n - 2$ oder weniger Variablen.[4]) Mit anderen Worten, die allgemeine Gleichung von höherem als siebentem Grade läßt sich auf ein Formenproblem von der Ordnung $n - 1$, aber nicht auf ein solches von niedrigerer Ordnung reduzieren. Einen klaren Bericht über diese und verwandte Gegenstände findet man in dem Wimanschen[5]) Enzyklopädie-Artikel I, 1, 1904, pp. 522—554.

---

1) Klein, Ikosaeder, 1884, pp. 211—260.

2) Klein, Math. Annalen 61, 1905, pp. 50—76 (Abdruck aus dem Journal für Math. 1905, pp. 151—174); Math. Abhandl. II, 1922, pp. 481—502.

3) Klein, Math. Annalen 28, 1887, pp. 499—532; Math. Abhandl. II, 1922, pp. 439—472.

4) Wiman, Math. Annalen 52, 1899, pp. 243—270.

5) Betr. neuerer Literatur vergleiche man: E. H. Moore, Math. Annalen 51, 1898—1899, pp. 417—444. Coble, ibid. 70, 1911, pp. 337—350; Trans. Amer. Math. Soc. 9, 1908, pp. 396—424; 12, 1911, pp. 311—325. Dickson, ibid. 9, 1908, pp. 121—148; 12, 1911, pp. 75—97. Speiser, Math. Annalen 77, 1916, pp. 546—562. Schur, Berl. Berichte 1908, pp. 664—678; Journal für Math. 127, 1904, p. 20; 132, 1907, p. 85; 139, 1911, pp. 155—164 (vgl. de Séguier, Journal de Math. (6), 6, 1910, pp. 387—436; 7, 1911, pp. 113—121). Weber, Algebra, 2. Ausg., 1899, II, pp. 228—301, 373—389, 470—550. Weber-Fricke, Algebra II, 1926.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

VIERZEHNTES KAPITEL.

DARSTELLUNG EINER ENDLICHEN GRUPPE ALS LINEARE GRUPPE. GRUPPENCHARAKTERE.

136. Einleitung. Als Fortsetzung des vorhergehenden Kapitels werden wir jetzt einige wichtige Sätze über die Darstellung einer Gruppe als lineare Gruppe beweisen und werden ferner eine Einführung in die Theorie der Gruppencharaktere geben. Diese Theorie ist unentbehrlich für endliche Gruppen und hat zu Sätzen geführt, welche sich auf andere Weise nicht beweisen ließen, so z. B. zu dem Satz, daß jede Gruppe von der Ordnung $p^a q^b$, wo p und q Primzahlen sind, auflösbar ist, oder zu dem Satz, daß jede transitive Gruppe vom Primzahlgrade entweder auflösbar oder zweifach transitiv ist.

Von einem einfachen, von Dedekind herrührenden Beispiel ausgehend, entwickelte Frobenius diese Theorie in einer Reihe schwer lesbarer Abhandlungen.[1]) Wir werden hier eine einfachere, von Schur[2]) herrührende Darstellung geben.

137. Reduzible lineare Gruppen. Im dreizehnten Kapitel hatten wir den Begriff der Gruppe linearer Transformationen kennengelernt. Die dort für nur zwei Variablen angestellten allgemeinen Überlegungen bleiben auch im Falle mehrerer Variablen bestehen. An Stelle einer linearen Transformation

---

1) Berl. Berichte 1896—1903. — Eine einfache Darlegung der Frobeniusschen Theorie gab der Verfasser in den Annals of Math. 4, 1902, pp. 25—49; ebenso eine Ausdehnung auf Gruppen von Transformationen mod. p in Trans. Amer. Math. Soc. 8, 1907, pp. 389—398; Bull. Amer. Math. Soc. 13, 1906—1907, pp. 477—488.

2) Berl. Berichte 1905, pp. 406—432. Molien bediente sich in seiner Abhandlung in den Sitzungsber. Naturf. Gesellsch. Dorpat 11, 1896, pp. 259 bis 288 der hyperkomplexen Zahlen. — Andere Darstellungen gaben Blichfeldt, Finite Collineation Groups, Univ. Chicago Press 1917, pp. 116—138; Miller, Blichfeldt, Dickson, Theory of Finite Groups, pp. 257—78; Burnside, Theory of Groups, 2. Ausg., 1911, pp. 243—371, 464—484, 499.

144. und die Beispiele stammen vom Verfasser.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

$$\begin{aligned} z_1' &= a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n \\ z_2' &= a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n \\ &\cdots\cdots\cdots\cdots\cdots \\ z_n' &= a_{n1}z_1 + a_{n2}z_2 + \cdots + a_{nn}z_n \end{aligned}$$

können wir auch ihr Äquivalent, nämlich ihre Matrix A, setzen. Bilden die linearen Transformationen eine Gruppe — eine sog. lineare Gruppe —, so gilt dasselbe für das System der zugehörigen Matrizen.

Es liege nun eine Gruppe von g nichtsingulären linearen Transformationen vor, deren Matrizen R sich sämtlich durch eine nicht singuläre $n$reihige Matrix P in Matrizen der Gestalt

$$P^{-1}RP = M_R = \begin{pmatrix} A_R & O \\ C_R & D_R \end{pmatrix}$$

überführen lassen, wo A_R und D_R quadratische Matrizen vom Grade a bzw. d sind, C_R eine da-Matrix und O eine Nullmatrix mit a Zeilen und d Spalten ist. (Es muß natürlich $a + d = n$ sein.) In diesem Falle heißt die Gruppe reduzibel. Der Name rührt daher, daß unter dem Einfluß von M_R von den Variablen $z_1, \ldots, z_n$ die a ersten nur unter sich transformiert werden. — Ist C_R für alle g Matrizen ebenfalls eine Nullmatrix, so heißt die Gruppe ganzreduziert, andernfalls halbreduziert.

Satz 1: Jede halbreduzierte endliche Gruppe ist mit einer ganzreduzierten äquivalent.[1])

Dazu haben wir zu zeigen, daß alle Matrizen M_R sich in Matrizen N_R transformieren lassen, wo

$$N_R = \begin{pmatrix} A_R & O \\ O & D_R \end{pmatrix}.$$

Da zunächst mit R und S auch RS in der Gruppe enthalten ist, so ist

$$M_{RS} = P^{-1}RSP = P^{-1}RP \cdot P^{-1}SP = M_R M_S.$$

D. h. es ist

$$A_{RS} = A_R A_S, \quad D_{RS} = D_R D_S \tag{1}$$

$$C_{RS} = C_R A_S + D_R C_S. \tag{2}$$

(Die Bestandteile A und D jeder Matrix bilden daher ebenfalls je eine Gruppe, welche mit der ursprünglichen Gruppe isomorph ist.)

1) Maschke, Math. Annalen 52, 1899, p. 363.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Man multipliziere (2) rechtsseitig mit A_S^{-1} und summiere über die g Werte von S. Da $A_S A_S^{-1} = A_{E_a}$ die a reihige Einheitsmatrix ist, so erhalten wir

$$\sum_S C_{RS} A_S^{-1} = g C_R + D_R \cdot gF, \quad \text{wo} \quad F = \frac{1}{g} \sum_S C_S A_S^{-1}.$$

In der ersten Summe ersetze man S durch $R^{-1}S$. Dann folgt aus (1)

$$\sum_S C_S A_S^{-1} A_R = gF A_R, \qquad \text{also}$$

$$F A_R = C_R + D_R F. \tag{3}$$

Für die unimodulare Matrix

$$Q = \begin{pmatrix} E_a & O \\ F & E_d \end{pmatrix}$$

gilt nun nach (3): $M_R Q = Q N_R$, wo N_R die obige Matrix ist. Demnach ist $Q^{-1} M_R Q = N_R$, d. h. M_R wird durch Q in eine Matrix der verlangten Form übergeführt.

138. Darstellungen einer Gruppe als lineare Gruppe. Gruppenmatrix.

$$R = \begin{pmatrix} \xi_1 \xi_2 \dots \xi_n \\ \eta_1 \eta_2 \dots \eta_n \end{pmatrix}, \quad S = \begin{pmatrix} \eta_1 \eta_2 \dots \eta_n \\ \zeta_1 \zeta_2 \dots \zeta_n \end{pmatrix}$$

seien zwei Substitutionen einer Gruppe. Ihnen kann man die Transformationen

$$r: \quad \xi_1 = \eta_1, \dots, \xi_n = \eta_n; \qquad s: \quad \eta_1 = \zeta_1, \dots, \eta_n = \zeta_n$$

zuordnen. RS ist dann die Transformation rs: $\xi_1 = \zeta_1, \dots, \xi_n = \zeta_n$ zugeordnet (vgl. 22.).

Satz 2: Jede Substitutionsgruppe von n Elementen ist einstufig isomorph zu einer linearen Gruppe von n Variablen. —

Eine Substitutionsgruppe kann zu mehreren linearen Gruppen einstufig oder mehrstufig isomorph sein. —

$s_1 = E, s_2, \dots, s_g$ seien die Substitutionen einer Gruppe G (oder die Elemente einer abstrakten Gruppe G). M_{s_i} $(i = 1, \dots, g)$ sei ein System f reihiger quadratischer Matrizen von der Beschaffenheit, daß nicht jedes M_{s_i} singulär ist[1]) und daß die M eine Gruppe bilden, d. h. daß

$$M_{s_i} M_{s_j} = M_{s_i s_j} \qquad (i, j = 1, \dots, g) \tag{4}$$

1) Diese von Schur nicht getroffene Veraussetzung vereinfacht einige Beweise.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Setzt man hier $j = 1$, so bekommt man $M_{s_i} \cdot (M_{s_1} - E) = 0$, d. h. $M_{s_1} = E$. Da ferner $M_{s_i} M_{s_{i-1}} = M_{s_1} = E$, so ist jedes M_{s_i} nichtsingulär.

Ein solches System linearer Transformationen mit den Matrizen $M_{s_1}, \ldots, M_{s_g}$ heißt eine **Darstellung** von G als lineare Gruppe. Sind die M nicht alle verschieden, so enthält die lineare Gruppe mehrfach vorkommende Transformationen und ist mehrstufig isomorph zu G.

Um alle M gleichzeitig zu behandeln, führen wir g unabhängige Variablen x_{s_i} $(i = 1, \ldots, g)$ ein und nennen die Matrix

$$X = \sum_{i=1}^{g} M_{s_i} x_{s_i} \tag{5}$$

die **Gruppenmatrix**, die zu der Darstellung von G als die lineare Gruppe $\{M_{s_1}, \ldots, M_{s_g}\}$ gehört.

Z. B. sei $s_1 = E$, $s_2 = (12)(34)$, $s_3 = (13)(24)$, $s_4 = (14)(23)$. Als Darstellung der Gruppe kann man jetzt die Matrizen nehmen

$$M_1 = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}, \quad M_{s_2} = \begin{pmatrix} 0&1&0&0\\ 1&0&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}, \quad M_{s_3} = \begin{pmatrix} 0&0&1&0\\ 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0 \end{pmatrix}, \quad M_{s_4} = \begin{pmatrix} 0&0&0&1\\ 0&0&1&0\\ 0&1&0&0\\ 1&0&0&0 \end{pmatrix}.$$

Die zugehörige Gruppenmatrix $M_1 x_1 + M_{s_2} x_2 + M_{s_3} x_3 + M_{s_4} x_4$ geht dann über in

$$X = \begin{pmatrix} x_1 & x_2 & x_3 & x_4\\ x_2 & x_1 & x_4 & x_3\\ x_3 & x_4 & x_1 & x_2\\ x_4 & x_3 & x_2 & x_1 \end{pmatrix}.$$

T bezeichne diejenige Transformation von der Matrix X, welche $\xi_1, \ldots, \xi_4$ linear durch $\eta_1, \ldots, \eta_4$ ausdrückt. Führt man die neuen Variablen

$$\begin{aligned} \zeta_1 &= \xi_1 + \xi_2 + \xi_3 + \xi_4, \quad \zeta_2 = \xi_1 + \xi_2 - \xi_3 - \xi_4,\\ \zeta_3 &= \xi_1 - \xi_2 + \xi_3 - \xi_4, \quad \zeta_4 = \xi_1 - \xi_2 - \xi_3 + \xi_4,\\ \omega_1 &= \eta_1 + \eta_2 + \eta_3 + \eta_4, \quad \omega_2 = \eta_1 + \eta_2 - \eta_3 - \eta_4,\\ \omega_3 &= \eta_1 - \eta_2 + \eta_3 - \eta_4, \quad \omega_4 = \eta_1 - \eta_2 - \eta_3 + \eta_4, \end{aligned}$$

ein, so geht T über in

$$\begin{aligned} \zeta_1 &= (x_1 + x_2 + x_3 + x_4)\,\omega_1\\ \zeta_2 &= (x_1 + x_2 - x_3 - x_4)\,\omega_2\\ \zeta_3 &= (x_1 - x_2 + x_3 - x_4)\,\omega_3\\ \zeta_4 &= (x_1 - x_2 - x_3 + x_4)\,\omega_4. \end{aligned}$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

139. Irreduzible Gruppenmatrizen. Ist X eine Gruppenmatrix und P eine nichtsinguläre konstante Matrix, so heißt $P^{-1}XP$ eine zu X äquivalente Gruppenmatrix.

Hilfssatz: Sind X und Y zwei irreduzible Gruppenmatrizen von den Ordnungen f und h und von der Beschaffenheit, daß $XP = PY$, wo P eine konstante fh-Matrix ist, so ist entweder $P = 0$ oder sonst $f = h$, und die Determinante von P ist $\neq 0$, so daß X und Y äquivalent sind.

Man nehme an, es sei $P \neq 0$. Dann ist P vom Range $r > 0$. Man setze $s = f - r$, $t = h - r$. Dann existieren nach 30. nichtsinguläre f- bzw. $h$reihige Matrizen A und B, für die

$$Q = APB = \begin{pmatrix} E_r & Z_{rt} \\ Z_{sr} & Z_{st} \end{pmatrix},$$

wo E_r die $r$reihige Einheitsmatrix bezeichnet, während Z_{rt} die Nullmatrix mit r Zeilen und t Spalten ist. Setzt man noch

$$AXA^{-1} = X_1 = \begin{pmatrix} X_{rr} & X_{rt} \\ X_{sr} & X_{st} \end{pmatrix},$$

$$B^{-1}YB = Y_1 = \begin{pmatrix} Y_{rr} & Y_{rt} \\ Y_{sr} & Y_{st} \end{pmatrix},$$

wo X_{rt} r Zeilen und t Spalten besitzt, usw., so ergibt sich

$$X_1Q = AXA^{-1}Q = AXPB = APYB = APBY_1 = QY_1,$$

d. h.
$$X_1Q = \begin{pmatrix} X_{rr} & Z_{rt} \\ X_{sr} & Z_{st} \end{pmatrix} = QY_1 = \begin{pmatrix} Y_{rr} & Y_{rt} \\ Z_{sr} & Z_{st} \end{pmatrix},$$

so daß $X_{sr} = 0$, $Y_{rt} = 0$. Für $s > 0$ oder $t > 0$ wäre nun X bzw. Y reduzibel, gegen die Voraussetzung. Demnach muß $s = t = 0$, $r = f = h$, $Q = E_f$. $P = A^{-1}QB^{-1}$ ist also eine nichtsinguläre quadratische Matrix. —

Folgerung: Jede konstante Matrix M, die mit einer irreduziblen Gruppenmatrix X von der Ordnung f vertauschbar ist, hat die Gestalt cE_f. —

Denn wenn c eine Wurzel von $|M - zE_f| = 0$ ist, so ist $P = M - cE_f$ eine konstante Matrix von verschwindender Determinante, für welche $XP = PX$, so daß $P = 0$ und daher $M = cE_f$. —

Zu unserem nächsten Satz brauchen wir einige neue Bezeichnungen: Ist R irgendeines der Elemente $s_1, \ldots, s_g$ der Gruppe G, so werden wir die (bisher mit M_R bezeichnete) entsprechende $f$reihige Matrix A_R einer Darstellung von G als lineare Gruppe

Digitized by Google Original from UNIVERSITY OF MICHIGAN

mit (a_{ijR}) bezeichnen. In einer anderen Darstellung von G entspreche R der $h$reihigen Matrix $B_R = (b_{pqR})$. — Nun gilt der

Satz 3: Ist

$$X = (x_{ij}) \qquad (i, j = 1, \ldots, f)$$

eine f-reihige irreduzible Gruppenmatrix, so erfüllen die Koeffizienten von

$$x_{ij} = \sum a_{ijR} x_R \qquad (R = s_1, \ldots, s_g)$$

die Beziehungen

$$(6) \qquad \sum_{R=s_1}^{s_g} a_{ijR^{-1}} a_{klR} = \frac{g}{f} \delta_{il} \delta_{jk} \qquad (i, j, k, l = 1, \ldots, f),$$

wo $\delta_{ii} = 1$, $\delta_{ij} = 0$ $(i \neq j)$. *Ist ferner*

$$Y = (y_{pq}) \qquad (p, q = 1, \ldots, h)$$

eine zweite irreduzible Gruppenmatrix von der Ordnung h, die zu derselben Gruppe G gehört und die zu X nicht äquivalent ist, so stehen die a_{ij} und die b_{pq} von

$$y_{pq} = \sum b_{pqR} x_R \qquad (R = s_1, \ldots, s_g)$$

in der Beziehung

$$(7) \qquad \sum_{R=s_1}^{s_g} a_{ijR^{-1}} b_{pqR} = 0 \qquad \begin{pmatrix} i, j = 1, \ldots, f \\ p, q = 1, \ldots, h \end{pmatrix}.$$

Für irgendwelche Elemente R und S aus G ist

$$A_R A_S = A_{RS}, \quad B_R B_S = B_{RS}.$$

$U = (u_{ij})$ sei nun eine $f$reihige quadratische Matrix mit willkürlichen, konstanten Elementen u_{ij}. Man transformiere sie mit allen Elementen A_R und bezeichne die Summe aller Transformierten mit V:

$$(8) \qquad V = \sum_{R=s_1}^{s_g} A_{R^{-1}} U A_R.$$

Dieses V ist mit allen seinen Konjugierten identisch, denn die Glieder in

$$A_{S^{-1}} V A_S = \sum_R A_{(RS)^{-1}} U A_{RS}$$

unterscheiden sich von denen in (8) nur durch ihre Anordnung. Demnach ist $VA_S = A_S V$ für alle A_S und also auch $XV = VX$.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Nach unserer Folgerung ist also $V = vE_f$, wo v nach (8) eine lineare homogene Funktion der u ist:

$$v = \sum_{j,k} c_{jk} u_{jk}.$$

Wieder nach (8) ist daher

$$\sum_R \sum_{j,k} a_{ijR^{-1}} u_{jk} a_{klR} = \delta_{il} v$$

identisch in den u für alle i, l. Daraus folgt, daß

$$\sum_R a_{ijR^{-1}} a_{klR} = \delta_{il} c_{jk} \qquad (i, j, k, l = 1, \ldots, f). \tag{9}$$

Setzt man hier $l = i$ und summiert über i von 1 bis f, so erhält man

$$\sum_R \sum_i a_{kiR} a_{ijR^{-1}} = f \cdot c_{jk}.$$

Nun ist aber wegen $A_R A_{R^{-1}} = A_E = E_f$ die Summe

$$\sum_i a_{kiR} a_{ijR^{-1}} = \delta_{kj}.$$

Durch Summierung von $R = s_1, \ldots, s_g$ erhält man die linke Seite der vorigen Gleichung, daher ist $f \cdot c_{jk} = g \cdot \delta_{kj}$. Durch diese Beziehung geht in der Tat (9) in (6) über.

Um die Behauptung (7) zu beweisen, setze man

$$Z = \sum_R A_{R^{-1}} W B_R,$$

wo $W = (w_{ip})$ eine fh-Matrix mit beliebigen konstanten Elementen ist. Wie oben ist $A_{S^{-1}} Z B_S = Z$, also $ZY = XZ$. Da X und Y nicht äquivalent sind, so ist nach dem Hilfssatz $Z = 0$, daher auch

$$\sum_R \sum_{j,p} a_{ijR^{-1}} w_{jp} b_{pqR} = 0 \qquad (i = 1, \ldots, f; q = 1, \ldots, h).$$

Da die w willkürlich sind, so besteht (7) zu Recht. —

Satz 4: Sind $X = (x_{ij})$, $Y = (y_{pq})$, ... irgendwelche irreduziblen, zur selben Gruppe $G = \{s_1, \ldots, s_g\}$ gehörenden Gruppenmatrizen von den Ordnungen $f, h, \ldots$ und sind keine zwei dieser Matrizen äquivalent, dann sind die $f^2 + h^2 + \cdots$ homogenen linearen Funktionen $x_{ij}, y_{pq}, \ldots$ der Variablen x_{s_i} voneinander linear unabhängig.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Denn wenn für Konstante $c, d, \ldots$

$$\sum_{i,j} c_{ij} x_{ij} + \sum_{p,q} d_{pq} y_{pq} + \cdots = 0$$

wäre, so wäre mit den Bezeichnungen von Satz 3

$$\sum_{i,j} c_{ij} a_{ijR} + \sum_{p,q} d_{pq} b_{pqR} + \cdots = 0.$$

Multipliziert man mit $a_{klR^{-1}}$ und summiert für $R = s_1, \ldots, s_g$, so ist nach (6) und (7)

$$\sum_{i,j} c_{ij} \delta_{il} \delta_{jk} = 0.$$

Diese Summe reduziert sich aber offenbar auf c_{lk}. Ähnlich folgt, daß $d_{pq} = 0$. —

Satz 5: Die Determinante einer irreduziblen Gruppenmatrix ist eine irreduzible Funktion der Variabeln x_{s_i}. Zwei irreduzible Gruppenmatrizen sind dann und nur dann äquivalent, wenn ihre Determinanten identisch sind.

Ist $X = (x_{ij})$ eine irreduzible Gruppenmatrix von der Ordnung f, so sind nach Satz 4 die x_{ij} linear unabhängige Funktionen der x_R. Führt man daher f^2 unabhängige Variablen u_{ij} ein, so sind (vgl. 32.) f^2 der x_R durch die f^2 Gleichungen $x_{ij} = u_{ij}$ als lineare homogene Funktionen der u_{ij} und der übrig bleibenden x_R ausdrückbar. Wäre nun die Determinante $|x_{ij}|$ ein Produkt zweier Polynome in den x_R, so zerfiele, wenn man die $g - f^2$ übrigen x_R gleich Null setzte, auch $d \equiv |u_{ij}|$ in ein Produkt von zwei Polynomen v, w in den u_{ij}. Nun ist aber eine Determinante, deren Elemente unabhängige Variabeln sind, bekanntlich irreduzibel. Denn da d in jeder Variablen u linear ist, so dürfen wir annehmen, daß v vom Grade Null und w vom Grade 1 in u_{11} ist. Nun enthält kein Glied der entwickelten Determinante d das Produkt von u_{11} mit einem Gliede u_{r1} der ersten Spalte. Infolgedessen fehlt u_{r1} in v, während es in w linear vorkommt. Da ferner auch $u_{rc} u_{r1}$ in d nicht vorkommt, so fehlt jedes u_{rc} in v, d. h. v ist lediglich ein Zahlenfaktor, aber kein Polynom.

Um den zweiten Teil unseres Satzes zu beweisen, bezeichne man zwei irreduzible, nichtäquivalente Gruppenmatrizen mit $X = (x_{ij})$ bzw. $Y = (y_{pq})$. Nach Satz 4 können wir dann die x_R so wählen, daß die x_{ij} und die y_{pq} vorgeschriebene Werte annehmen. Daher sind die Determinanten von X und Y nicht identisch.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

140. Reduzible Gruppenmatrizen. Die wiederholte Anwendung von Satz 1 zeigt, daß eine reduzible Gruppenmatrix X in eine Gruppenmatrix

$$Y = \begin{pmatrix} Y_1 & 0 & \dots & 0 & 0 \\ 0 & Y_2 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 & Y_m \end{pmatrix} \tag{10}$$

übergeführt werden kann, wo jetzt jedes Y_i irreduzibel ist.

Satz 6: Jede Gruppenmatrix ist einer solchen vom Typus Y in (10) äquivalent. —

Nun ist eine solche Reduktion auf mehrere Arten und Weisen möglich. Es ist von vornherein nicht abzusehen, in welcher Beziehung zwei derartige Zerlegungen Y und Z mit den irreduziblen Komponenten $Y_1, \dots, Y_m$ bzw. $Z_1, \dots, Z_n$ zueinander stehen. Um dies zu untersuchen, stellen wir zunächst fest, daß nach Satz 5 die Determinanten d_i und D_i von Y_i bzw. Z_i irreduzibel sind. Da andererseits

$$d_1 d_2 \dots d_m \equiv D_1 D_2 \dots D_n$$

und da ein Polynom nur auf eine einzige Art und Weise in irreduzible Polynome zerlegbar ist, so muß $m = n$ sein und die d_i müssen, abgesehen von der Anordnung und abgesehen von Zahlenfaktoren, gleich den D_k sein. Nun reduziert sich aber für $x_E = 1$, $x_R = 0$ $(R \neq E)$ die Determinante einer Gruppenmatrix auf 1. Demnach können die erwähnten Zahlenfaktoren alle nur gleich 1 sein. Nach dem letzten Teil von Satz 5 sind daher die Matrizen Y_i abgesehen von der Reihenfolge äquivalent zu den Z_k.

Satz 7[1]: Die Zerlegung einer Gruppenmatrix in irreduzible Komponenten ist, wenn man äquivalente Komponenten als identisch betrachtet, eindeutig.

Sind auch von den Komponenten $Y_1, \dots, Y_m$ mehrere äquivalent, so können auch sie als identisch angenommen werden. Kommt Y_i genau r_i mal vor, so heißt r_i der Index von Y_i, und die Gesamtheit der r heißt die Indexreihe von Y oder X. —

Satz 8: Ist $X = (x_{ij})$ eine Gruppenmatrix mit der Indexreihe $r_1, \dots, r_l$ und sind $f_1, \dots, f_l$ die Ordnungen ihrer irreduziblen Komponenten, so sind genau $f_1^2 + \dots + f_l^2$ der Funktionen x_{ij} (der

1) Eine Verallgemeinerung dieses Satzes gab Loewy, Trans. Amer. Math. Soc. 4, 1903, p. 44.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Variablen x_R) linear unabhängig. Ferner ist $r_1^2 + \cdots + r_l^2$ gleich der Zahl v der linear unabhängigen, konstanten, mit X vertauschbaren Matrizen P. Endlich ist l gleich der Zahl w der linear unabhängigen, konstanten Matrizen, die mit X und allen P vertauschbar sind.

$Y_1, \ldots, Y_m$ seien die irreduziblen Komponenten von X bzw. Y. Dann folgt der erste Teil unseres Satzes sofort aus Satz 4. Um die anderen Behauptungen zu beweisen, bezeichnen wir die Y_i so, daß die ersten r_1 einander gleich sind, ferner die nächsten r_2 wieder gleich sind, usw.

Die Zahlen v und w bleiben ungeändert, wenn wir X mit Y vertauschen. Jede Matrix P können wir in der Form schreiben

$$P = \begin{pmatrix} P_{11} & P_{12} & \ldots & P_{1m} \\ \cdot & \cdot & \cdot & \cdot \\ P_{m1} & P_{m2} & \ldots & P_{mm} \end{pmatrix},$$

wo die Matrix P_{ij} aus t_i Zeilen und t_j Spalten besteht. Damit dann $YP = PY$, ist notwendig und hinreichend, daß

$$Y_i P_{ij} = P_{ij} Y_j \qquad (i, j = 1, \ldots, m).$$

Sind Y_i und Y_j nicht gleich und daher auch nicht äquivalent, so ist nach dem Hilfssatz $P_{ij} = 0$. Sind sie aber gleich (dies trifft r_1 bzw. r_2 bzw. r_3 usw. Mal zu), so zeigt die Folgerung in 139., daß $P_{ij} = cF_i$, wo $F_i = E_{t_i}$ die Einheitsmatrix von der Ordnung $t_i = t_j$ ist. Daher ist

$$P = \begin{pmatrix} c_{11}F_1 & \ldots & c_{1r_1}F_1 & 0 & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c_{r_1 1}F_1 & \ldots & c_{r_1 r_1}F_1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & d_{11}F_{r_1+1} & \ldots & d_{1r_2}F_{r_1+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots & 0 & d_{r_2 1}F_{r_1+1} & \ldots & d_{r_2 r_2}F_{r_1+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

Umgekehrt zeigt ihre Entstehung, daß jede solche Matrix P mit X vertauschbar ist. Die Zahl der willkürlichen Parameter $c_{ij}, d_{kn}, \ldots$, ist aber $v = r_1^2 + r_2^2 + \cdots + r_l^2$.

Bezeichnet Q schließlich eine konstante, mit X und allen P vertauschbare Matrix, so kann es, da es mit X vertauschbar ist, aus P hergeleitet werden, indem man die $c, d, \ldots$ durch $C, D, \ldots$ ersetzt. Da Q mit allen P vertauschbar sein soll, so muß auch die

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Matrix (C_{ij}) mit allen Matrizen (c_{ij}), (D_{kn}) mit allen (d_{kn}) usw. vertauschbar sein. (C_{ij}), (D_{kn}), ... sind daher bis auf Zahlenfaktoren gleich den Einheitsmatrizen von den Ordnungen $r_1, r_2, \ldots$. Diese Bedingungen reichen auch dafür hin, daß Q mit X und allen P vertauschbar ist. Die Zahl w der willkürlichen Parameter von Q ist offenbar gleich l.

141. Die reguläre Gruppenmatrix. Die zwischen den Elementen einer Gruppe $G = \{s_1 = E, \ldots, s_g\}$ bestehenden Beziehungen lassen sich am einfachsten in einer sog. Gruppen- oder Multiplikationstafel zusammenfassen. Man schreibt dazu in die erste Zeile die Elemente s_i von G, in die zweite Zeile die Elemente $s_i s_2$ von Gs_2, usw. Dadurch erhält man eine quadratische Tafel, die einem das Produkt $s_i s_j$ als Element s_l der $i$ten Spalte und $j$ten Zeile liefert. Als Beispiel führen wir die Matrix X von 138. an, in der man nur x durch s zu ersetzen hat, um eine Multiplikationstafel zu bekommen. Ändere ich die Tafel ein wenig um, indem ich in die $i$te Zeile $j$te Spalte das Element $s_i s_j^{-1}$ setze (was nur auf eine veränderte Multiplikation herauskommt) und führe ich wieder unabhängige Variabeln x mit jenen Indizes $s_i s_j^{-1}$ ein, so erhalte ich eine mit G verbundene $g$reihige quadratische Matrix X, die das Aussehen einer Gruppenmatrix $\sum M_s x_s$ — summiert über alle Elemente s von G — hat, wenn man unter M_s diejenige Matrix versteht, deren Element σ_{ij} in der $i$ten Zeile $j$ten Spalte gleich 1 oder 0 ist, je nachdem $s_i s_j^{-1} = s$ oder $\neq s$. Es muß aber noch nach (4) $M_s M_t = M_{st}$ für alle Matrizen M_i sein, damit wirklich eine Gruppenmatrix vorliegt. Bezeichnet man die Elemente von M_t mit τ_{jk} (welche wiederum nur die Werte 1 oder 0 annehmen können, je nachdem $s_j s_k^{-1} = t$ oder $\neq t$), so sind die Elemente von $M_s M_t$ gleich $\pi_{ik} = \sum_j \sigma_{ij}\tau_{jk}$. Jedes Produkt $\sigma\tau$ ist nur dann von Null verschieden, und zwar gleich 1, wenn

$$s_i s_j^{-1} = s, \quad s_j s_k^{-1} = t.$$

Daraus folgt, daß in diesem Falle $s_i s_k^{-1} = st$. Besteht letztere Gleichung nicht, so ist also $\pi_{ik} = 0$. Ist sie aber erfüllt, so ist das einzige nichtverschwindende Glied von π_{ik} dasjenige, für welches j durch $s_j = t s_k$ bestimmt ist, und es ist dann $\pi_{ik} = 1$. Die aus den π_{ik} bestehende Matrix ist demnach gleich M_{st}. D. h. es ist $M_s M_t = M_{st}$. Da auch noch $M_{s_1} = M_E$ die $g$reihige Einheitsmatrix ist, so haben wir

Satz 9: X ist eine zu G gehörige Gruppenmatrix, die sog. reguläre Gruppenmatrix.

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Ist G eine reguläre Substitutionsgruppe (92.), so führt die in 138. gezeigte Darstellung von G als lineare Gruppe auf unsere gegenwärtigen Matrizen M_{s_i}. —

Satz 10: Man bezeichne die irreduziblen Komponenten einer regulären Gruppenmatrix X mit X_i, so daß keine zwei der $X_1, \ldots, X_c$ äquivalent sind, während jede andere Komponente einer von diesen äquivalent ist. Hat dann X_i die Ordnung f_i und den Index e_i, so ist $f_i = e_i$ für jedes i und c ist die Anzahl der Klassen konjugierter Elemente der Gruppe G.

Durch Zählen der Zeilen erhält man

$$e_1 f_1 + \cdots + e_c f_c = g.$$

Da jedes Element von X eine der g Variablen x ist, so ist nach dem ersten Teil von Satz 8

$$f_1^2 + \cdots + f_c^2 = g.$$

Nun sei Y eine von den x unabhängige Matrix; das Element der $i$ten Zeile $j$ten Spalte bezeichne man mit $[s_i, s_j]$. Greift man das Element der $i$ten Zeile $k$ten Spalte aus XY und YX heraus, so sieht man, daß X und Y dann und nur dann vertauschbar sind, wenn identisch in den x

$$\sum_j x_{s_i s_j^{-1}} [s_j, s_k] \equiv \sum_t [s_i, s_t] x_{s_t s_k^{-1}} \qquad (i, k = 1, \ldots, g).$$

Die beiden x haben nun gleiche Indizes, wenn $s_t = s_i s_j^{-1} s_k$. Die Koeffizienten andererseits sind gleich, wenn

$$[s_j, s_k] = [s_i, s_i s_j^{-1} s_k] \qquad (i, k, j = 1, \ldots, g).$$

Führt man s_n mittels der Gleichung $s_i = s_n s_j$ ein, so muß also

$$[s_j, s_k] = [s_n s_j, s_n s_k] \qquad (j, k, n = 1, \ldots, g).$$

Für $[s_i, s_1]$ schreibe man y_{s_i}, dann ist nach Obigem

$$y_{s_j^{-1} s_i} = [s_j^{-1} s_i, s_1] = [s_i, s_j] \quad \text{und} \quad Y = (y_{s_i^{-1} s_i}).$$

Da demnach Y die g unabhängigen Parameter y enthält, so ist nach dem zweiten Teil von Satz 8

$$e_1^2 + \cdots + e_c^2 = g.$$

Mit Hilfe der früheren Beziehungen folgt daraus

$$(e_1 - f_1)^2 + \cdots + (e_c - f_c)^2 = g - 2g + g = 0,$$

d. h. es ist $e_i = f_i$ für alle i.

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Eine von den x unabhängige, mit X vertauschbare Matrix Z ist notwendigerweise vom Typus Y. Da $X = (x_{s_i^{-1}s_j})$, $Y = (y_{s_j^{-1}s_i})$, X und Y sich also in den Indizes lediglich durch die Reihenfolge der Faktoren unterscheiden, so ist umgekehrt jede mit Y vertauschbare Matrix vom Typus X. Demnach ist eine Matrix Z dann und nur dann sowohl mit X als auch mit jedem Y vertauschbar, wenn das Element der $i$ten Zeile $j$ten Spalte gleichzeitig die Typen Y und X besitzt, d. h. wenn

$$z_{s_j^{-1}s_i} = z_{s_i s_j^{-1}} \qquad (i, j = 1, \ldots, g).$$

Setzt man also $s_j^{-1}s_i = s$, so ist zur Gleichheit $z_s = z_t$ notwendig und hinreichend, daß $t = s_j s s_j^{-1}$, d. h. daß s und t unter G konjugiert sind. Nach der Schlußbehauptung von Satz 8 ist daher die Zahl c der unabhängigen Parameter in Z gleich der Klassenzahl konjugierter Elemente von G. —

Es könnte sein, daß es eine zu G gehörende irreduzible Gruppenmatrix H von der Ordnung h gibt, die zu keiner der c irreduziblen Komponenten $X_1, \ldots, X_c$ der regulären Gruppenmatrix äquivalent ist. Dann zeigt der erste Teil von Satz 8, daß es in der Gruppenmatrix (x_{ij}), welche die irreduziblen Komponenten $X_1, \ldots, X_c, H$ hat,

$$f_1^2 + \cdots + f_c^2 + h^2 = g + h^2$$

linear unabhängige Funktionen x_{ij} von $x_{s_1}, \ldots, x_{s_g}$ gibt, während offenbar doch nicht mehr als g Funktionen linear unabhängig sein können. Damit haben wir

Satz 11: Die Gesamtzahl der zu einer Gruppe G gehörenden, irreduziblen Gruppenmatrizen, von denen keine zwei einander äquivalent sind, ist gleich der Zahl c der Klassen konjugierter Elemente von G.

142. Gruppencharaktere. Wir gehen aus von einer Darstellung von $G = \{s_1 = E, s_2, \ldots, s_g\}$ als Gruppe linearer Transformationen mit den nichtsingulären Matrizen M_{s_i}. Die Spuren — d. h. die Summe der Diagonalelemente — der letzteren bezeichne man mit $\chi(s_i)$. Das System von g Zahlen $\chi(s_1), \ldots, \chi(s_g)$ heißt ein zu dieser Darstellung oder zu der entsprechenden Gruppenmatrix $X = \sum M_{s_i} x_{s_i}$ gehörender Charakter von G.

So ist für die vierreihige Gruppenmatrix X des Beispiels in 138. $\chi(s_1) = 4$, $\chi(s_2) = \chi(s_3) = \chi(s_4) = 0$. — Wir sahen, daß $\zeta_2 = z\omega_2$, wo

$$z = x_1 + x_2 - x_3 - x_4.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Verwenden wir diese neue Gruppenmatrix (z), die nur das einzige Element z enthält, so bekommen wir den neuen Charakter

$$\chi(s_1) = \chi(s_2) = 1, \quad \chi(s_3) = \chi(s_4) = -1.$$

Da ähnliche Matrizen dieselbe Spur haben, so haben äquivalente Darstellungen oder äquivalente Gruppenmatrizen denselben Charakter. Nach Satz 11 gibt es dann irreduzible Gruppenmatrizen $X_1, \ldots, X_c$ — von denen keine zwei äquivalent sind —, derart daß jede irreduzible Gruppenmatrix einer von diesen äquivalent ist. Die zugehörigen Charaktere seien $\chi_1(s_i), \ldots, \chi_c(s_i)$.

Wenn X_j unter den irreduziblen Komponenten der Gruppenmatrix X genau $r_j$mal $(r_j \geqq 0)$ vorkommt, so ist offenbar

$$\chi(s_i) = r_1\chi_1(s_i) + \cdots + r_c\chi_c(s_i). \quad (11)$$

—

Sind u und v zwei bestimmte Zahlen des Systems $1, \ldots, c$, so setze man

$$X_u = \sum_{R=s_1}^{s_g} (a_{ijR})\, x_R, \quad X_v = \sum_{R} (b_{pqR})\, x_R \quad \begin{pmatrix} i, j = 1, \ldots, f_u \\ p, q = 1, \ldots, f_v \end{pmatrix}.$$

Dann ist $$\chi_u(R) = \sum_i a_{iiR}, \quad \chi_v(R) = \sum_p b_{ppR}.$$

Ersetzt man in (6) i durch m und k durch n, multipliziert die entstehende Gleichung mit $a_{imS}b_{knT}$ und summiert für $m, n = 1, \ldots, f$, so erhält man

$$\sum_R \sum_{m=1}^{f} a_{imS}a_{mjR^{-1}} \cdot \sum_{n=1}^{f} a_{knT}a_{nlR} = \frac{g}{f} \sum_{m,n} \delta_{ml}\delta_{jn}a_{imS}a_{knT}.$$

Der Summand auf der rechten Seite verschwindet, außer wenn $m = l$, $n = j$. Da ferner $A_S A_R{}^{-1} = A_{SR^{-1}}$, so können wir die Summationen links ausführen und erhalten

$$\sum_R a_{ijSR^{-1}}a_{klTR} = \frac{g}{f} a_{ilS}a_{kjT}. \quad (12)$$

Aus (7) erhalten wir auf die gleiche Weise

$$\sum_R a_{ijSR^{-1}}b_{pqTR} = 0. \quad (13)$$

Jetzt setze man in (12) $j = i$, $l = k$, $T = E$:

$$\sum_R a_{iiSR^{-1}}a_{kkR} = \frac{g}{f} a_{ikS}\delta_{ki}.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

Summiert man über i und k und fügt den Index u hinzu, so folgt

$$\sum_R \chi_u(SR^{-1})\chi_u(R) = \frac{g}{f_u}\chi_u(S). \tag{14}$$

Da $\chi_u(E) = f_u$, so ergibt sich für den Fall $S = E$

$$\sum_R \chi_u(R^{-1})\chi_u(R) = g. \tag{15}$$

Setzt man ähnlich in (13) $j = i$, $q = p$, $T = E$ und summiert über i und p, so bekommt man

$$\sum_R \chi_u(SR^{-1})\chi_v(R) = 0 \qquad (u \neq v). \tag{16}$$

Wir kehren jetzt zur allgemeinen Gruppenmatrix X zurück, welcher der Charakter $\chi(s_i)$ für $s_i = 1, \ldots, g$ entspricht. Multipliziert man (11) mit $\chi_u(s_i^{-1})$ und summiert über i von 1 bis g, so folgt

$$\sum_{i=1}^{g} \chi(s_i)\chi_u(s_i^{-1}) = \sum_{v=1}^{c} \sum_{i=1}^{g} r_v \chi_v(s_i)\chi_u(s_i^{-1}).$$

Aus (16) folgt für $S = E$, daß für $v \neq u$ die innere Summe der rechten Seite verschwindet. Für $v = u$ ist sie nach (15) gleich $r_u g$. Demnach ist r_u durch die Werte von $\chi(s_i)$ und die festen Zahlen $\chi_u(s_i^{-1})$ bestimmt. Nun gibt aber r_j an, wie oft X_j als irreduzible Komponente von X vorkommt. Damit sind wir zu dem Satz gelangt:

Satz 12: Zwei Darstellungen von G als lineare Gruppen sind dann und nur dann äquivalent, wenn sie dieselben Charaktere haben.

143. Anwendungen auf Gruppenmatrizen. G sei eine kommutative Gruppe und $X = \sum M_{s_i} x_{s_i}$ sei eine zugehörige irreduzible Gruppenmatrix von der Ordnung f. Da jedes M mit X vertauschbar ist, so ist es nach der Folgerung von 139. von der Form $c_i E_f$. Ist s_i von der Ordnung e_i, so ist $M^{e_i} = E_f$, d. h. c_i ist eine $e_i$te Einheitswurzel. Für $f > 1$ wäre $X = \sum (c_i x_{s_i}) E_f$ eine reduzible Matrix.

Satz 13: Eine irreduzible Gruppenmatrix, die einer kommutativen Gruppe entspricht, ist von der Ordnung 1.

Vgl. das Beispiel am Ende von 138.

Aus Satz 6 folgt, daß jede Darstellung einer kommutativen Gruppe $g$ter Ordnung in eine Darstellung übergeführt werden

Digitized by Google Original from UNIVERSITY OF MICHIGAN

kann, deren Matrizen als Diagonalelemente $g$te Einheitswurzeln haben und deren andere Elemente verschwinden. Diese Eigenschaft gilt also insbesondere für zyklische Gruppen, und so haben wir

Satz 14: Die Spur jeder linearen Transformation endlicher Ordnung ist eine Summe von Einheitswurzeln. —

Satz 15: Die Ordnung einer irreduziblen Gruppenmatrix von G ist ein Teiler der Ordnung g von G.

Unter F_s verstehe man 1 oder 0, je nachdem $s = E$ oder $\neq E$. Dann ist

$$\sum_R \chi(R) F_{SR^{-1}} = \chi(S),$$

so daß (14) die Form annimmt

$$\sum_R \chi(R) \left\{ \frac{g}{f} F_{SR^{-1}} - \chi(SR^{-1}) \right\} = 0.$$

Da $\chi(E) = f \neq 0$, so ist die Determinante

$$\left| \frac{g}{f} F_{SR^{-1}} - \chi(SR^{-1}) \right| = 0 \qquad (R, S = s_1, \ldots, s_g).$$

Wie wir sahen, ist die Spur χ von SR^{-1} eine Summe von Einheitswurzeln und daher eine ganze algebraische Zahl. Daher ist $\frac{g}{f}$ eine Wurzel einer Gleichung vom Grade g, deren Leitglied gleich 1 ist und deren übrige Koeffizienten ganze algebraische Zahlen sind. Demnach ist sie selbst eine ganze algebraische Zahl und, da sie gleichzeitig rational ist, eine ganze (rationale) Zahl, d. h. g ist durch f teilbar.

144. Die alternierende Gruppe G von 5 Elementen. Nach Beispiel 5 von 113. hat G genau 5 Komplexe konjugierter Substitutionen. Die 5 Darstellungen von G als irreduzible lineare Gruppe (vgl. Satz 10) mögen die Ordnungen 1, a, b, c, d haben. Nach Satz 15 sind sie alle Teiler von 60, und nach Satz 8 ist ihre Quadratsumme gleich 60. Die Maximalordnung ist offenbar 6. Für $d = 6$ wird aber $a^2 + b^2 + c^2 = 23$, was keine ganzzahlige Lösung hat. Für $d = 5$ wird $a^2 + b^2 + c^2 = 34$. Setzt man hier $c = 5$, so ist $a^2 + b^2 = 9$, d. h. entweder a oder b ist gleich Null. Setzt man aber $c = 4$, so wird $a = b = 3$. Die a, b, c sind also nicht alle $\leqq 3$. Sind endlich a, b, c, d alle $\leqq 4$, so sind sie keinesfalls alle $= 4$, während andererseits $1^2 + 4^2 + 4^2 + 3^2 = 58 < 60$.

Satz 16: Jede Darstellung der alternierenden Gruppe von 5 Elementen als irreduzible lineare Gruppe ist äquivalent zu einer solchen

Digitized by Google Original from UNIVERSITY OF MICHIGAN

von 1, 3, 4 oder 5 Variablen, wobei es im Falle dreier Variabeln zwei verschiedene Typen gibt.

145. Berechnung von Gruppencharakteren. In (12) setze man $k = j$, $l = i$ und summiere über i und j; so bekommt man

$$f \sum_R \chi(S R^{-1} T R) = g \chi(S) \chi(T). \tag{17}$$

Da $A_R A_S$ und $A_S A_R$ dieselben Spuren haben, so ist

$$\chi(RS) = \chi(SR) \tag{18}$$

oder, wie man durch Ersetzen von R durch $S^{-1}R$ bekommt, $\chi(S^{-1}RS) = \chi(R)$. —

Nehmen wir nun die symmetrische Gruppe von 3 Elementen und setzen

$$A = (132),\ B = (123),\ C = (12),\ D = (13),\ F = (23).$$

Die drei Komplexe von Konjugierten sind E; A, B; C, D, F. Nach (18) ist daher

$$\chi(A) = \chi(B), \qquad \chi(C) = \chi(D) = \chi(F).$$

Verwendet man (17) für $T = E$, so wird $\chi(E) = f$; verwendet man es für $S = T = A$ bzw. $S = T = C$ bzw. $S = A$, $T = C$ und berücksichtigt (15), so ergibt sich

$$3f^2 + 3f \cdot \chi(A) = 6\chi^2(A) \qquad 2f^2 + 4f \cdot \chi(A) = 6\chi^2(C)$$
$$6f \cdot \chi(C) = 6\chi(A) \cdot \chi(C) \qquad f^2 + 2\chi^2(A) + 3\chi^2(C) = 6.$$

Für $\chi(C) \neq 0$ gibt die dritte Beziehung $\chi(A) = f$, und die anderen Beziehungen geben dann $\chi^2(C) = f^2 = 1$. Da f als Ordnung der Gruppenmatrix positiv ist, so haben wir

$$f = 1, \quad \chi(E) = \chi(A) = 1, \quad \chi(C) = \pm 1.$$

Für $\chi(C) = 0$ reduzieren sich die Bedingungen auf $\chi(A) = -\frac{1}{2}f$, $f^2 = 4$, so daß

$$f = 2, \quad \chi(E) = 2, \quad \chi(A) = -1, \quad \chi(C) = 0.$$

Digitized by Google Original from UNIVERSITY OF MICHIGAN

SACHVERZEICHNIS.

Die Zahlen beziehen sich auf die Seiten.

Abhängigkeit, lineare 49
Adjunktion 146
Alternierende Form 73. 111
  Funktion 143
  Gruppe 143
Annihilator 23. 25
Assoziatives Gesetz 2. 41. 137

Bereich s. Körper

Determinante 45
  charakteristische 44. 84. 92
  Funktional- 5
  s. Form, Matrix, Transformation
Diskriminante
  e. biquadrat. Form 140
  e. kubischen Form 6. 8. 16. 135
  e. quadratischen Form 4. 6. 16
Distributives Gesetz 42
Drehungen 89—91. 196
Dreiteilung des Winkels 191. 193

Einheitswurzeln 150. 151
Elementarteiler 98

Form 2
  alternierende 73. 111
  bilineare 47 (s. Matrix)
  biquadratische 17. 18 bis 20
  definite 66
Form, fünft. Ordnung 35
  Hermitesche 60—79
  Hessesche 2. 5. 6. 21
  Jacobische 5. 22
  kanonische 8. 14. 34 bis 36. 64. 78
  kubische 6. 8. 16. 133—136
  lineare 37—57
  positive 66, 67
  quadratische 58—79. 65. 66
    Index 64—78
  Rang s. Matrix
  Reduktion 62. 74—78
  Signatur 70
  symmetrische 58—79
Formenpaare 101—131
  im singulären Falle 115—131
  Weierstraßsche- 112
Formenproblem 209 bis 214
Funktion, alternierende 143
  gehörig zu einer Gruppe 161
  konjugierte 162
  Wertigkeit 153

Gewicht s. Invariante, Kovariante
Gleichung, auflösbare 168—190. 169. 181. 185. 187
  biquadratische 18 bis 20. 139
Gleichung, charakteristische 43
  fünften Grades 219. 221
  Hauptgl. 215. 217
  Ikosaeder- 220
  irreduzible 148
  Kreisteilungsgl. 150. 179
  kubische 8. 133—136
  lineare homogene 55
    inhomogene 56
  Resolventen- 169. 170
  reziproke 140
  Wurzeln 147
  zyklische 178
Gruppe, allgemeine 140 bis 141
  alternierende 143. 175. 187. 238
  auflösbar 177
  Charakter 235—239
  Darstellung 225
  Durchschnitt 142. 144
  einfache 175
  Erzeugende 140. 142
  Faktor- 175
  Galoissche Gr. einer Gleichung 152—190. 156—158. 165
    Erniedrigung 164
  gehörig zu einer Gr. 142. 161
  Ikosaeder- 206—209
  Index 144
  kommutative 142. 177
  konjugierte 173

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Gruppe, lineare 223—239
Monodromie- 166
Oktaeder- 204—205
Ordnung 140. 144
Polyeder- 196—222
Quotienten- 175
reduzible 223
reguläre 158. 174
Substitutionsgruppe 133—144. 140. 141
symmetrische 140
Tetraeder- 198—203
transitive 158
Untergruppe 140. 144. 173
invariante 173. 176. 177
eigentliche 176
Valentiner- 222
zusammengesetzte 175
zyklische 174. 177. 179
Gruppenmatrix 226 bis 235. 237—238

Harmonische Lage 6. 22
Homogen 2. 9. 26

Index 144
-reihe 176
Invariante 1—36. 4. 11. 20—21
absolute 18
Gewicht 4. 10. 11
numerische 20
Seminvariante 12 bis 18. 27. 35
vollständiges System 15—18. 30—33
Invariante Faktoren 88. 93. 94
Irreduzibel 148. 150
Isobar 11. 25. 26
Isomorph 171

Kommutator 26
komplexe Zahlen, höhere 49
Kompositionsreihe 176
konjugierte Funktion 162
Körper 48. 145
Adjunktion 146. 164
Kovariante 1—36. 4. 22. 25
Gewicht 4. 10. 11
Hessesche s. Form
Jacobische s. Form
Kanonizante 35
Leitglied 11. 12. 13. 15—18. 27
vollständiges System 15—18. 30—33

Leitglied 11. 12. 13. 15 bis 18. 27

Matrix 36. 47. 131 bis 132
Äquivalenz 52. 59. 101
charakteristische 43
Division v. Matrizen 42
Hermitesche 60—79, 70
kongruente 59
Multiplikation 38. 42 (s. Transformation)
Rang 45. 59. 70—74
schiefsymmetrische 73
Summe 42
symmetrische 58. 70
transponierte 48
verschwisterte 60
Wurzeln einer 107
Matrizenpaare s. Formenpaare
Minimalgradzahlen 127. 128

Polygone, reguläre 194

Quaternion 43. 99—100

Reduzibilität 148
Resolvente 139
Galoissche 154

Spezieller Punkt 202. 205. 208
Substitution 135. 136
grade 143
identische 138
induzierte 135
invariante 175
inverse 138
Ordnung 136
positive 143
Potenz 138
Produkt 136
-sgruppe s. Gruppe
transformierte 174
Symbolik 33. 36
Syzygie 17. 33

Teiler, größter gemeinsamer 146
teilerfremd 147
Trägheitsgesetz 65
Transformation, adjungierte 39
ähnliche 93
Determinante 39
identische 2. 40
inverse 2. 40. 42
involutorische 62
kanonische Form, rationale 80—84
klassische 94
lineare 1. 14. 20. 37. 80—100
orthogonale 66. 69. 70 89—91
Produkte 1. 39. 42
projektive 20—22
singuläre 39
skalare 40. 42
s. Substitution 174
Tschirnhausen- 215
unitäre 69

Zyklus 135. 138

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

NAMENVERZEICHNIS.

Die Zahlen beziehen sich auf die Seiten.

Abel 168. 169
Aronhold 21. 22. 36

Baker 166
Bauer 166
Berwick 190
Bianchi 166. 219
Blichfeldt 166. 167. 176. 223
Börger 166
Brioschi 190. 214
Bucca 183
Burckhardt 196

Cayley 17. 19. 33. 36. 37. 91
Clebsch 22. 36
Coble 222
Coolidge 147

Dedekind 223
Descartes 192
Dickson 36. 49. 100. 101. 111. 115. 131. 132. 166. 167. 176. 190. 193. 222. 223

Euler 5. 26. 168

Faà di Bruno 20
Frobenius 101, 112. 132. 166
Furtwängler 166

Galois 152. 169. 185
Gauß 149. 191
Gordan 6. 22

Hamilton 168
Hermite 166
Hesse 2. 6. 22
Hilbert 28. 165
Hölder 176. 183
Hurwitz 100. 131. 166

Jacobi 5
Jordan 176. 183

Klein 196. 219. 222
Kneser 166. 183
König 166
Kowalewski 80
Kronecker 74. 112. 115
Krull 80

Lagrange 163. 179
Landsberg 183
Lattès 80
Liouville 152
Loewy 92. 167. 183. 231

Maillet 166
Maschke 224
Miller 166. 167. 176. 223
Molien 223
Moore 222
Muth 92. 111. 112. 115

Noether 6. 166

Palatini 36
Pascal 91
Petersen 193
Picard 167

Reye 36
Ritt 166
Rosanes 36
Ruffini 168. 169

Schur 166. 222. 223
de Séguier 222
Serret 168
Speiser 176, 222
Study 22

Terracini 36
Tschirnhaus 215

Vessiot 167

Wantzel 168. 193
Weber 147. 166. 167. 222
Weisner 166
Weitzenböck 36
Wiman 222

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Arithmetik und Algebra nebst den Elementen der Differentialrechnung. Von Dr. *E. Borel,* Prof. a. d. Sorbonne Paris. Vom Verfasser genehmigte deutsche Ausgabe besorgt von Geh. Hofrat Dr. *P. Stäckel,* weil. Prof. a. d. Univ. Heidelberg. 2. Aufl. Mit 56 Textfig. u. 3 Taf. [XVI u. 404 S.] 8. 1919. (Elemente der Mathematik Bd. I.) Geh. ℳ 12.—, geb. ℳ 14.—

Die Grundlehren der Arithmetik und Algebra. Bearb. von Geh. Hofrat Dr. *E. Netto,* weil. Prof. a. d. Univ. Gießen, u. Dr. *C. Färber,* weil. Oberrealschulprof., Berlin. (Grundlehren der Mathematik I. Teil.)

I. Band: Arithmetik. Von *C. Färber.* Mit 9 Fig. [XV u. 410 S.] gr. 8. 1911. Geb. ℳ 14.—

II. Band: Algebra. Von *E. Netto.* [XII u. 232 S.] gr. 8. 1915. Geb. ℳ 7.80

Elementare Algebra. Akadem. Vorlesungen für Studierende der ersten Semester. Von Geh. Hofrat Dr. *E. Netto,* weil. Prof. a. d. Univ. Gießen. 2. Aufl. Mit 19 Fig. i. T. [X u. 200 S.] gr. 8. 1913. Geh. ℳ 6.—, geb. ℳ 8.—

Vorlesungen über Algebra. Unter Benutzung der dritten Auflage des gleichnamigen Werkes von † Dr. G. Bauer. In 4., verm. Aufl. dargest. von Dr. *L. Bieberbach,* Prof. a. d. Univ. Berlin. Mit 16 Fig. i. T. u. auf 1 Taf. [X u. 334 S.] gr. 8. 1928. Geb. ℳ 20.—

Das Buch hält auch in der neuen Bearbeitung von Prof. Bieberbach an dem Ziel der Bauerschen Ausgabe fest, eine für die Zwecke der Lehramtskandidaten bestimmte Einführung in die Algebra zu liefern, und will daher nicht die Algebra in einer ‚splendid isolation' von den übrigen Gebieten der Mathematik, sondern gerade in Fühlung mit denselben aufbauen. Im Mittelpunkt steht wieder die Theorie der algebraischen Gleichungen. Prof. Bieberbach hat bei der Neubearbeitung sein Bestreben dahin gerichtet, nach Stoff und Form der Darstellung dem heutigen Stand der Wissenschaft gerecht zu werden. Neu hinzugefügte Abschnitte betreffen u. a. die graphische Auflösung von Gleichungen, die mannigfachen Sätze über die Lage der Gleichungswurzeln und die Galoissche Gleichungstheorie.

Einführung in die höhere Algebra. (Introduction to higher algebra.) Von Dr. *M. Bôcher,* Prof. a. d. Havard-Univ. zu Cambridge. Deutsch von Dr. *H. Beck,* Prof. a. d. Univ. Bonn. Mit einem Geleitwort von Geh. Reg.-Rat Dr. *E. Study,* Prof. a. d. Univ. Bonn. 2. Aufl. [XII u. 348 S.] gr. 8. 1925. Geb. ℳ 13.50

Einleitung in die allgemeine Theorie der algebraischen Größen. Von Prof Dr. *W. König,* Budapest. [X u. 564 S.] gr. 8. 1903. Geb. ℳ 22.—

Pascals Repertorium der höheren Mathematik. 2., völlig umgearb. Aufl. der deutschen Ausgabe. Unt. Mitw. zahlr. Mathematiker hrsg. von Dr. *E. Salkowski,* Prof. a. d. Techn. Hochschule in Berlin, u. Dr. *H. E. Timerding,* Prof. a. d. Techn. Hochschule in Braunschweig.

I. Band: Analysis. Hrsg. von *E. Salkowski.*

1. Teilband: Algebra, Differential- und Integralrechnung. [XV u. 527 S.] gr. 8. 1910. Geb. ℳ 18.—

2. Teilband: Differentialgleichungen, Funktionentheorie. Mit 26 Fig. i. T. [XII u. S. 529—1023.] gr. 8. 1927. Geb. ℳ 18.—

3. Teilband: Reelle Funktionen, Neuere Entwicklungen, Zahlentheorie. Mit Fig. gr. 8. 1929. Geb. ℳ 22.—

II. Band: Geometrie. Hrsg. von *H. E. Timerding.*

1. Teilband: Grundlagen und ebene Geometrie. Mit 54 Fig. [XVIII u. 534 S.] gr. 8. 1910. Geb. ℳ 18.—

2. Teilband: Raumgeometrie. Mit 12 Fig. i. T. [XII u. 628 S.] gr. 8. 1922. Geh. ℳ 17.—, geb. ℳ 20.—

Verlag von B. G. Teubner in Leipzig und Berlin

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Lehrbuch der Funktionentheorie. Von Dr. *W. F. Osgood*, Prof. a. d. Harvard-Univ. Cambridge, Mass. (Teubn. Lehrbücher d. math. Wissensch. Bd. XX, 1—3)

I. Band. 5. Aufl. Mit 174 Fig. [XIV u. 818 S.] gr. 8. 1928. Geh. *RM* 42.—, geb. *RM* 44.—

II. Band. 1. Liefg. 2. Aufl. Mit 6 Fig. [VIII u. 307 S.] gr. 8. 1929. Geh. *RM* 16.—, geb. *RM* 18.—. **2. Liefg.** [In Vorb. 1929]

Das Buch gibt eine systematische Entwicklung der komplexen Funktionentheorie auf Grundlage der Infinitesimalrechnung und in engster Fühlung mit der Geometrie und der mathematischen Physik. Im ersten Bande wird unter Zugrundelegung von Sätzen über reelle Funktionen und Mengenlehre die Cauchysche Theorie entwickelt. Es folgen die Riemannschen Flächen nebst der konformen Abbildung und die Theorie der analytischen Funktionen, sowie deren Anwendung auf periodische Funktionen, Reihen- und Produktenentwicklungen. Den Schluß bildet eine Behandlung des logarithmischen Potentials und der Uniformisierung algebraischer und allgemeiner Funktionen.

Lehrbuch der Funktionentheorie. Von Dr. *L. Bieberbach*, Prof. a. d. Univ. Berlin.

I. Band: Die Elemente der Funktionentheorie. 2., verb. Aufl. Mit 80 Fig. i. T. [VI u. 314 S.] gr. 8. 1923. Geb. *RM* 15.—

II. Band: Moderne Funktionentheorie. Mit 44 Fig. i. T. [VII u. 366 S.] gr. 8. 1927. Geb. *RM* 20.—

Vorlesungen über reelle Funktionen. Von Dr. *C. Carathéodory*, Prof. a. d. Univ. München. 2. Aufl. Mit 47 Fig. i. T. [X u. 718 S.] gr. 8. 1927. Geh. *RM* 27.—, geb. *RM* 29.—

„Es ist ein Werk aus einem Guß, das vieles Neue und Eigenartige enthält. Viele vom Verfasser eingeführte Begriffe und Ergebnisse werden zweifellos zum dauernden Besitz der Wissenschaft werden. Es ist ein wertvolles Geschenk, das uns Carathéodory mit diesem tiefdurchdachten Werk beschert hat."

(Jahrbuch über die Fortschritte der Mathematik.)

Praktische Analysis. Von Dr. *H. v. Sanden*, Prof. a. d. Techn. Hochschule in Hannover. 2., verb. Aufl. Mit 32 Abb. i. T. [XVIII u. 195 S.] 8. 1923. (Handb. d. ang. Math. 1.) Kart. *RM* 5.60

Zahlenrechnen. Von Dr. *L. von Schrutka*, Prof. a. d. Univ. Wien. [X u. 146 S.] 8. 1923. (Samml. math.-phys. Lehrb. Bd. 20.) Kart. *RM* 4.40

Praktische Infinitesimalrechnung. Von *F. F. P. Bisacre*, M. A. (Chartered Civil Engeneer), Ascania Helensburgh. Deutsch von Dr. *E. Treffitz*, Prof. a. d. Techn. Hochschule in Dresden, u. Dr. phil. *E. König*, Elberfeld. Mit 104 Abb. u. 3 Taf. [XII u. 364 S.] 8. 1929. Geh. *RM* 16.—, geb. *RM* 18.—

Das Buch gibt eine Einführung in die Infinitesimalrechnung etwa in dem Umfange, der dem Unterricht im ersten Semester an unseren Technischen Hochschulen entspricht (Koordinaten, Funktionen, Grenzwerte, Differentiation, Integration einfacher Funktionen, einfachste Differentialgleichungen). Es wendet sich in erster Linie an solche Studierenden der Naturwissenschaften und Technik, „die sich die Fähigkeit erwerben wollen, die Infinitesimalrechnung praktisch zu handhaben." Dementsprechend enthält es in besonders ausführlicher Darstellung eine reiche Auswahl von Anwendungen aus der Mechanik, der Elektrizitätslehre, der physikalischen Chemie und der Thermodynamik.

Partielle Differentialgleichungen. Deutsche Ausgabe von *Webster*, Partial Differential Equations. Hrsg. von Dr. *G. Szegö*, Prof. a. d. Univ. Königsberg/Pr. (Teubn. Lehrb. d. math. Wiss. Bd. XLIII.) [U. d. Pr. 1929]

Integralgleichungen unter besonderer Berücksichtigung der Anwendungen. Von Dr. *G. Wiarda*, Prof. a. d. Techn. Hochschule i. Dresden. (Samml. math.-phys. Lehrb. Bd. 25.) [In Vorb. 1929]

Verlag von B. G. Teubner in Leipzig und Berlin

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

In „Teubners mathematischen Leitfäden" sind erschienen:

Mathematisches Praktikum. Von Dr. *H. v. Sanden,* Prof. an der Techn. Hochschule in Hannover. (Bd. 27/28.)

I. Teil. Mit 17 Fig. i. T. sowie 20 Zahlentaf. als Anhang. [V u. 122 S.] 8. 1927. Geb. *RM* 6.80

II. Teil. [U. d. Pr. 1929]

Der vorliegende erste Band setzt nur die Grundbegriffe der Differential- und Integralrechnung voraus und behandelt den Rechenschieber, den Lehrsatz von Taylor, die Auflösung algebraischer und transzendenter Gleichungen, die Ausgleichsrechnung, die numerische Integration und Differentiation sowie die Zerlegung und Zusammensetzung periodischer Funktionen. Die wichtigsten mathematischen Grundlagen sind jeweils kurz zusammengestellt und die Aufgaben selbst unter sorgfältiger Genauigkeitsdiskussion bis zur letzten Zahl durchgerechnet. Ein zweiter Band ist in Vorbereitung und soll in gleicher Weise die gewöhnlichen Differentialgleichungen behandeln.

Höhere Mathematik für Mathematiker, Physiker und Ingenieure. Von Dr. *R. Rothe,* Prof. a. d. Techn. Hochschule in Berlin. (Bd. 21—23.)

I. Teil: Differentialrechnung und Grundformeln der Integralrechnung nebst Anwendungen. 2. Aufl. Mit 155 Fig. i. T. [VII u. 186 S.] 8. 1927. Kart. *RM* 6.—

II. Teil: Integralrechnung, Unendliche Reihen, Vektorrechnung nebst Anwendungen. Mit 96 Fig. i. T. [VIII u. 201 S.] 8. 1929. Kart. *RM* 6.40

III. Teil: Raumkurven und Flächen, Linienintegrale und mehrfache Integrale, gewöhnliche und partielle Differentialgleichungen nebst Anwendungen. [In Vorb. 1929]

Mit diesem Werke soll ein das Gesamtgebiet der höheren Mathematik umfassender entsprechend den Grundsätzen der Sammlung knapp gehaltener Leitfaden in freier Anordnung des Stoffes, aber mit zahlreichen Beispielen, Anwendungen und Übungen geboten werden. Der jetzt bereits in 2. Auflage vorliegende erste Band enthält einen einleitenden Abschnitt über Zahlen, Veränderliche und Funktionen, behandelt sodann die Hauptsätze der Differentialrechnung und die Grundformeln der Integralrechnung, Funktionen von zwei und mehr Veränderlichen, Differentialgeometrie ebener Kurven, komplexe Zahlen, Veränderliche und Funktionen. Der zweite Band bringt die Begründung und die üblichen Verfahren der Integralrechnung, die Theorie und Praxis der unendlichen Reihen, Linienintegrale und Integrale in Komplexen sowie einiges über Determinanten und Vektorrechnung.

Differential- und Integralrechnung. Von Dr. *L. Bieberbach,* Prof. a. d. Univ. Berlin. (Bd. 4 u. 5.)

I. Teil: Differentialrechnung. 3., verm. und verb. Aufl. Mit 34 Fig. [VI u. 142 S.] 8. 1928. Geb. *RM* 5.40

II. Teil: Integralrechnung. 3., verm. und verb. Aufl. Mit 25 Fig. [IV u. 150 S.] 8. 1928. Kart. *RM* 5.80

Funktionentheorie. Von Dr. *L. Bieberbach,* Prof. a. d. Univ. Berlin. Mit 34 Fig. i. T. [IV u. 118 S.] 8. 1922. (Bd. 14.) Kart. *RM* 3.20

Einführung in die Vektoranalysis, mit Anwendungen auf die mathematische Physik. Von Dr. *R. Gans,* Prof. a. d. Univ. Königsberg. 5., verb. Aufl. Mit 40 Fig. [VI u. 120 S.] 8. 1923. (Bd. 16.) Kart. *RM* 3.—

Analytische Geometrie. Von Geh. Hofrat Dr. *R. Fricke,* Prof. a. d. Techn Hochschule in Braunschweig. 2. Aufl. Mit 96 Fig. [VI u. 135 S.] 8. 1922. (Bd 1.) Kart. *RM* 3.60

Darstellende Geometrie. Von Dr. *M. Großmann,* Prof. a. d. Eidgen. Techn. Hochschule in Zürich. (Bd. 2 u. 3.)

I. Teil. 2., erw. Aufl. Mit 134 Fig. u. 100 Übungsaufgaben. [VI u. 81 S.] 8. 1922. Kart. *RM* 2.20.

II. Teil. 2., erw. Aufl. Mit 144 Fig. [VI u. 154 S.] 8. 1921. Kart. *RM* 4.—

Verlag von B. G. Teubner in Leipzig und Berlin

Digitized by Google
Original from UNIVERSITY OF MICHIGAN

Sammlung mathematisch-physikalischer Lehrbücher

Herausgegeben von Dr. E. Trefftz

Prof. a. d. Techn. Hochschule in Dresden

Zahlenrechnen. Von Dr. L. von Schrutka, Prof. a. d. Techn. Hochschule in Wien. [X u. 146 S.] Kart. ℳ 4.40 . . . . . (Bd. 20.)

Einführung in die Wahrscheinlichkeitsrechnung. Von J. L. Coolidge, Prof. a. d. Harvard Univ. Cambridge U. S. A. Deutsch von Dr. Fr. M. Urban, Brünn. [IX u. 212 S.] Geb. ℳ 10.— (Bd. 24.)

Integralgleichungen unter besonderer Berücksichtigung der Anwendungen. Von Dr. G. Wiarda, Prof. a. d. Techn. Hochsch. in Dresden. [U. d. Presse 1929] . . . . . (Bd. 25.)

Die Determinanten. Von Geh. Hofrat Dr. E. Netto, weil. Prof. a. d. Univ. Gießen. 2., verb. Aufl. von Dr. L. Bieberbach, Prof. a. d. Univ. Berlin. [VI u. 123 S.] Kart. ℳ 4.40 . . (Bd. 9.)

Theorie der elliptischen Funktionen. Von weil. Geh. Hofrat Prof. Dr. M. Krause, unter Mitwirkung von Dr. E. Naetsch, Prof. a. d. Techn. Hochsch. in Dresden. Mit 25 Fig. [VII u. 186 S.] Kart. ℳ 5.40 . . . . . (Bd. 13.)

Die Theorie der Besselschen Funktionen. Von Prof. Dr. P. Schafheitlin, Berlin. Mit 1 Figurentafel. [V. u. 129 S.] Kart. ℳ 4.— . . . . . (Bd 4.)

Das Lebesguesche Integral. Eine Einführung in die neuere Theorie der reellen Funktionen. Von Dr. E. Kamke, Prof. a. d. Univ. Tübingen. Mit 9 Fig. im Text. [V u. 151 S.] Kart. ℳ 7.— (Bd. 23)

Konforme Abbildung. Von Dr. L. Lewent, weil. Oberlehrer in Berlin. Hrsg. von Geh. Bergrat Dr. E. Jahnke, weil. Prof. a. d. Techn. Hochschule in Berlin. Mit Beitrag von Dr. W. Blaschke, Prof. a. d. Univ. Hamburg. Mit 40 Abb. [VI u. 118 S.] Kart. ℳ 3.80 . . . . . (Bd. 14.)

Funktionentafeln mit Formeln und Kurven. Von Geh. Bergrat Dr E. Jahnke, weil. Prof. a. d. Techn. Hochsch. in Berlin und F. Emde, Prof. a. d. Techn. Hochsch. in Stuttgart. Mit 53 Textfig. [XII u. 176 S.] Geb. ℳ 8.— . . . . . (Bd. 5.)

Graphische Methoden. Von Geh. Reg.-Rat Dr. C. Runge, weil. Prof. a. d. Univ. Göttingen. 3. Aufl. Mit 94 Fig. im Text. [IV u. 130 S.] Geb. ℳ 5.40 . . . . . (Bd. 18.)

Theorie der Kräftepläne. Von Dr. H. E. Timerding, Prof. a. d. Techn. Hochsch. in Braunschweig. Mit 46 Fig. [VI u. 99 S.] Kart. ℳ 3.— . . . . . (Bd. 7.)

Die Vektoranalysis und ihre Anwendung in der theoretischen Physik. Von Dr. W. v. Ignatowsky, Prof. a. d. Univ. Leningrad. I. Die Vektoranalysis. 3., umgeänd. Aufl. Mit 27 Textfig. [VIII u. 110 S.] II. Anwendung der Vektoranalysis in der theoret. Physik. 3., neubearb. Aufl. Mit 14 Textfig. [IV u. 120 S.] Kart. je ℳ 5.60 . . . . . (Bd. 6, 1. u. 2.)

Die ebene Vektorrechnung und ihre Anwendungen in der Wechselstromtechnik. Von Dr.-Ing. H. Kafka in Ladowitz bei Dux. Teil I: Grundlagen. Mit 62 Fig. i. T. [VIII u. 132 S.] Kart. ℳ 7.—. Teil II: Besondere Anwendung in der Wechselstromtechnik. [In Vorb. 1929] (Bd. 22, 1u. 2.)

Das Rechnen mit symmetrischen Komponenten. Ein Lehrbuch für Elektrotechniker. Von Ing. Dr. techn. G. Oberdorfer, Privatdoz. a. d. Techn Hochschule in Wien. [In Vorb. 1929] (Bd. 26.)

Einführung in die Theorie des Magnetismus. Von Dr. R. Gans, Prof. a. d. Univ. Königsberg. Mit 40 Fig. [VI u. 110 S.] Kart. ℳ 3.20 . . . . . (Bd. 1.)

Einführung in die Maxwellsche Theorie der Elektrizität und des Magnetismus. Von Dr. Cl. Schaefer, Prof. a. d. Univ. Breslau. 3. Aufl. Mit Bildnis J. C. Maxwells und 33 Textfig. [VI u. 174 S.] Geb. ℳ 6.60 . . . . . (Bd. 3.)

Grundzüge der mathematisch-physikalischen Akustik. Von Dr. A. Kalähne, Prof. a. d. Techn. Hochschule in Danzig. 2 Teile. I. Teil: [VII u. 144 S.] Kart. ℳ 4.—. II. Teil: Mit 57 Fig. im Text. [X u. 225 S.] Kart. ℳ 6.80 . . . . . (Bd. 11, 1 u. 2.)

Einführung in die kinetische Theorie der Gase. Von Dr. A. Byk. Prof. a. d. Univ. u. d. Techn. Hochsch. in Berlin. I. Teil: Die idealen Gase. Mit 14 Fig. [V u. 102 S.] Kart. ℳ 3.— (Bd. 10.)

Dispersion und Absorption des Lichts inruhenden isotropen Körpern. Theorie und ihre Folgerungen. Von Dr. D. A. Goldhammer, Prof. a. d. Univ. Kasan. Mit 28 Fig. [VI u. 144 S.] Kart. ℳ 4.40 . . . . . (Bd. 16.)

Die Theorie der Wechselströme. Von Geh. Reg.-Rat Dr. E. Orlich, Prof. a. d. Techn. Hochschule in Berlin. Mit 37 Fig. [IV u. 94 S.] Kart. ℳ 3.— . . . . . (Bd. 12.)

Elektromagnetische Ausgleichsvorgänge in Freileitungen und Kabeln. Von Dr. Dr.-Ing. h. c. K. W. Wagner, Prof. a. d. Techn. Hochsch. in Berlin. Mit 23 Fig. [IV u. 109 S.] Kart. ℳ 3.20 (Bd. 2.)

Die mathematischen Instrumente. Von Geh. Reg.-Rat Dr. A. Galle, Prof. am Geodät. Institut in Potsdam. Mit 86 Abb. [VI u. 187 S.] Kart. ℳ 5.60 . . . . . (Bd. 15.)

Mathematische Theorie der astronomischen Finsternisse. Von Prof. Dr. P. Schwahn, weil. Dir. d. Ges. u. Sternwarte „Urania" in Berlin. Mit 20 Fig. [VI u. 128 S.] Kart. ℳ 3.80 (Bd. 8.)

Elemente der technischen Hydromechanik. Von Dr. Dr.-Ing. R. v. Mises, Prof. a. d. Univ. Berlin. I. Teil. Mit 72 Fig. im Text. [VIII u. 212 S.] Kart. ℳ 6.—. [II. In Vorb. 1929] (Bd. 17, 1 u. 2.)

Graphische Hydraulik. Von Dr.-Ing. A. Schoklitsch, Prof. a. d. deutschen techn. Hochschule in Brünn. Mit 45 Fig. im Text u. auf 2 Tafeln. [IV u. 72 S.] Kart. ℳ 2.60 . . . . . (Bd. 21.)

VERLAG VON B. G. TEUBNER IN LEIPZIG UND BERLIN

Digitized by Google
Original from UNIVERSITY OF MICHIGAN